Updated: 26/12/2014

Finite fields

Michel Waldschmidt

http://www.math.jussieu.fr/~miw/articles/pdf/FiniteFields2013.pdf

Contents

1 Background

Among many references for this preliminary section are D.S. Dummit & R.M. Foote [3] and S. Lang [5].

1.1 Group theory

Groups, subgroups. Lagrange's theorem: *the order of a subgroup of a finite group divides the order of the group.* Index of a subgroup in a group.

Additive vs multiplicative notation.

Abelian groups (=commutative groups).

Intersection of subgroups. Subgroup generated by a subset. Finitely generated group. Subgroup generated by an element.

The *order* of an element is the order of the subgroup generated by this element. An element x in a multiplicative group G is *torsion* if it has finite order, that means if there exists $m \geq 1$ such that $x^m = 1$. In this case the order of x is the least of these integers m's. The set of $m \in \mathbf{Z}$ with $x^m = 1$ is a subgroup of $\mathbf{Z}$ which is not 0, hence, it has a unique positive generator d, which is *the order of* x. Therefore, for an element x of order d, we have

$$x^m = 1 \Longleftrightarrow d|m.$$

We stress that the condition $x^m = 1$ does not mean that x has order m, it means that the order of x divides m.

If x is an element in a multiplicative group G and m an integer such that $x^m = 1$, then for i and j in $\mathbf{Z}$ satisfying $i \equiv j \bmod m$ we have $x^i = x^j$. In other terms, the kernel of the morphism

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ j & \mapsto & x^j \end{array}$$

contains $m\mathbf{Z}$. Hence, this morphism factors to $\mathbf{Z}/m\mathbf{Z} \longrightarrow G$, which we denote again by $j \mapsto x^j$. This means that we define x^j for j a class modulo m by selecting any representative of j in $\mathbf{Z}$.

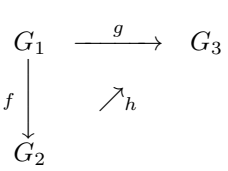
The *torsion subgroup* of a commutative group. *Exponent* of a torsion group G: the smallest integer $m \geq 1$ such that $x^m = 1$ for all $x \in G$. Examples of torsion groups: in additive notation $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Q}/\mathbf{Z}$. In multiplicative notation: n-th roots of unity, group of all roots of unity in $\mathbf{C}$.

Direct product and *direct sum* of groups (this is the same when there are only finitely many groups).

Morphisms (also called *homomorphisms*) between groups. Isomorphisms, *endomorphisms*, *automorphisms*. *Kernel* of a morphism. *Quotient* of a group by a subgroup.

Theorem of factorisation for morphisms of groups.

Given an surjective morphism of groups $f : G_1 \longrightarrow G_2$ and a morphism of groups $g : G_1 \longrightarrow G_3$, there exists a morphism $h : G_2 \longrightarrow G_3$ such that $h \circ f = g$ if and only if $\ker f \subset \ker g$.



If h exists, then h is surjective if and only if g is surjective, and h is injective if and only if $\ker f = \ker g$.

Example: $G_2 = G_1/H$ when G_1 is abelian, H a subgroup of G_1, and f is the canonical morphism.

Cyclic groups. The subgroups and quotients of a cyclic group are cyclic. For any cyclic group of order n and for any divisor d of n, there is a unique subgroup of G of order d; if ζ is a generator of the cyclic group G of order n and if d divides n, then $\zeta^{n/d}$ has order d, hence, is a generator of the unique subgroup of G of order d. In a cyclic group whose order is a multiple of d, there are exactly d elements whose orders are divisors of d, and these are the elements of the subgroup of order d. In a cyclic group G of order a multiple of d, the set of elements $\{x^d \mid x \in G\}$ is the unique subgroup of G of index d.

A direct product $G_1 \times G_2$ is cyclic if and only if G_1 and G_2 are cyclic with relatively prime orders.

The number of generators of a cyclic group of order n is $\varphi(n)$, where φ is Euler's function (see § 1.4.1).

1.2 Ring theory

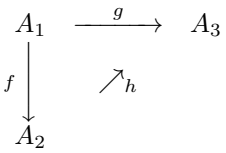
Unless otherwise explicitly specified, the rings are commutative, with a unity 1 and $1 \neq 0$. Often, they have no zero divisors (they are called *domains*), but not always: indeed, we will consider quotient rings like $\mathbf{Z}/n\mathbf{Z}$ where n is not a prime number.

Characteristic of a ring.

Intersection of rings. For B a ring, A a subring and E a subset of B, the ring generated by E over A is denoted by $A[E]$. Special case where $E = \{\alpha_1, \ldots, \alpha_n\}$: we denote it by $A[\alpha_1, \ldots, \alpha_n]$.

Morphisms between rings, *isomporhisms*, *endomorphisms*, *automorphisms*. *Ideal* of a ring, *kernel* of a morphism. *Quotient* of a commutative ring by an ideal $\mathcal{I} \neq \{0\}$. Canonical morphism $A \to A/\mathcal{I}$. *Prime ideals, maximal ideals.*

Theorem of factorisation for morphisms of rings. *Given a surjective morphism of rings $f : A_1 \longrightarrow A_2$ and a morphism of rings $g : A_1 \longrightarrow A_3$, there exists a morphism $h : A_2 \longrightarrow A_3$ such that $h \circ f = g$ if and only if* $\ker f \subset \ker g$.



If h exists, then h is surjective if and only if g is surjective, and h is injective if and only if $\ker f = \ker g$.

Example: $A_2 = A_1/\mathcal{I}$ when A_1 is commutative, $\mathcal{I}$ an ideal of A_1, and f is the canonical morphism.

Quotient field of a domain.

The ring of polynomials in one variable $A[X]$ or in several variables $A[X_1, \ldots, X_n]$.

The *units* of a ring A are the invertible elements, they form a multiplicative group $A^\times$. A *field* is a ring F such that $F^\times = F \setminus \{0\}$. The torsion elements in the group $A^\times$ are the *roots of unity* in A. Their set

$$A^\times_{\text{tors}} = \{x \in A \mid \text{ there exists } n \geq 1 \text{ such that } x^n = 1\}$$

is the *torsion subgroup* of the group of units $A^\times$.

Euclidean rings, principal rings, factorial rings. Examples: $\mathbf{Z}$, $k[X]$ where k is a field, $A[X]$ where A is a ring, $k[X_1, \ldots, X_n]$ and $A[X_1, \ldots, X_n]$.

Given two rings A_1, B_2, a subring A_2 of B_2, a morphism of rings

$$f : A_1 \to A_2 \subset B_2$$

and elements $y_1, \ldots, y_n$ of B_2, there is a unique morphism

$$F : A_1[X_1, \ldots, X_n] \to A_2[y_1, \ldots, y_n]$$

such that $F(a) = f(a)$ for $a \in A_1$ and $F(X_i) = y_i$ for $1 \leq i \leq n$.

As a consequence, if $f : A_1 \to A_2$ is a morphism of rings, there is a unique morphism of rings $A_1[X_1, \ldots, X_n] \to A_2[X_1, \ldots, X_n]$ which coincides with f on A_1 and maps X_i to X_i for $1 \leq i \leq n$.

A fundamental example is the surjective morphism of rings

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X], \tag{1}$$

which maps X to X and $\mathbf{Z}$ onto $\mathbf{F}_p$ by reduction modulo p of the coefficients. Its kernel is the principal ideal $p\mathbf{Z}[X] = (p)$ of $\mathbf{Z}[X]$ generated by p.

Exercise 2. Given two rings B_1, B_2, a subring A_1 of B_1, a subring A_2 of B_2, a morphism of ring $f : A_1 \to A_2$,

$$\begin{array}{ccc} B_1 & & B_2 \\ \cup & & \cup \\ A_1 & \xrightarrow[f]{} & A_2 \end{array}$$

elements $x_1, \ldots, x_n$ of B_1 and elements $y_1, \ldots, y_n$ of B_2, a necessary and sufficient condition for the existence of a morphism $F : A_1[x_1, \ldots, x_n] \to A_2[y_1, \ldots, y_n]$ such that $F(a) = f(a)$ for $a \in A_1$ and $F(x_i) = y_i$ for $1 \leq i \leq n$ is the following:

For any polynomial $P \in A_1[X_1, \ldots, X_n]$ *such that*

$$P(x_1, \ldots, x_n) = 0,$$

the polynomial $Q \in A_2[X_1, \ldots, X_n]$*, image of* P *by the extension of* f *to* $A_1[X_1, \ldots, X_n] \to A_2[X_1, \ldots, X_n]$*, satisfies*

$$Q(y_1, \ldots, y_n) = 0.$$

Modules over a ring. *Example*: **Z**–modules are nothing else than the abelian groups.

Structure theorem for finitely generated modules over a principal ring. *Application*: structure theorems for finitely generated abelian groups and for finite groups. *Rank* of a finitely generated abelian group.
Consequence: In a finite abelian group of exponent e, there exists an element of order e.

1.3 Field theory

The characteristic of a field K is either 0 or else a prime number p. In the first case, the *prime field* (smallest subfield of K, which is the intersection of all subfields of K) is $\mathbf{Q}$; in the second case, it is $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.

Intersection of fields. If L is a field and K a subfield, we say that L is an *extension of* K. Then L is a K–vector space. Further, if E is a subset of L, we denote by $K(E)$ the field generated by E over K: it is the quotient field of $K[E]$. If $E = \{\alpha_1, \ldots, \alpha_n\}$, we write $K(E) = K(\alpha_1, \ldots, \alpha_n)$. If K_1 and K_2 are two subfields of a field L, the *compositum* of K_1 and K_2 is the subfield field $K_1(K_2) = K_2(K_1)$ of L generated by $K_1 \cup K_2$.

A morphism $f : K \to A$, where K is a field and A a ring, is injective.

When L_1 and L_2 are two extensions of K, a *K-morphism* $L_1 \to L_2$ is a field morphism whose restriction to K is the identity. If $f : L_1 \to L_2$ is a field morphism, then L_1 and L_2 have the same characteristic, hence, the same prime field F, and f is a F–morphism.

If L is an extension of K, the K–automorphisms of L form a group denoted $\mathrm{Aut}(L/K)$.

Finitely generated extensions. *Algebraic* and *transcendental* extensions.

Finite extensions, degree $[L : K]$. For $K_1 \subset K_2 \subset K_3$, we have

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1].$$

Given an extension $L \supset K$ of fields and an element $\alpha \in L$, there is a unique map $K[X] \to K[\alpha]$, which is the identity on K and maps X to α. Kernel of this map. *Irreducible* (monic) polynomial of an algebraic element over a field K. The field $K[X]/(f) = K(\alpha)$ when α is algebraic over K.

For L an extension of K, an element α in L is algebraic over K if and only if $K[\alpha] = K(\alpha)$, and this is true if and only if $[K(\alpha) : K]$ is finite.

Splitting field of a polynomial over a field. *Algebraic closure* of a field. Two algebraic closures of K are K–isomorphic, but, usually, there is no unicity of such a morphism (since there are many K–automorphisms of the algebraic closure: they constitute the *absolute Galois group* of K).

An element α in an algebraically closed extension Ω of a field K is algebraic over K if and only if the set of $\sigma(\alpha)$, where σ ranges over the K–automorphisms of Ω, is finite.

Given an algebraically closed field Ω, a subfield K of Ω and an element $\alpha \in \Omega$ algebraic over K, the roots in Ω of the irreducible polynomial f of α over K are the *conjugates* of α over K. If $\alpha_1, \ldots, \alpha_m$ are the distinct roots of f in Ω, then there are exactly m K–morphisms $K(\alpha) \to \Omega$, say $\sigma_1, \ldots, \sigma_m$, where σ_i is determined by $\sigma_i(\alpha) = \alpha_i$.

Zeroes of polynomials: *multiplicity* or *order* of a zero of a polynomial in one variable.

1.4 Arithmetic

1.4.1 Residue classes modulo n

Subgroups of $\mathbf{Z}$. Morphism $s_n : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$. There exists a morphism $\varphi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ such that $\varphi \circ s_a = s_b$ if and only if $a\mathbf{Z} \subset b\mathbf{Z}$, which means if and only if b divides a. If φ exists, then φ is unique and surjective. Its kernel is $b\mathbf{Z}/a\mathbf{Z}$ which is isomorphic to $\mathbf{Z}/(a/b)\mathbf{Z}$.

The *greatest common divisor* $gcd(a, b)$ of a and b is the positive generator of $a\mathbf{Z}+b\mathbf{Z}$, the *least common multiple* $\mathrm{lcm}(a, b)$ of a and b is the positive generator of $a\mathbf{Z} \cap b\mathbf{Z}$.

The order of the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ of the ring $\mathbf{Z}/n\mathbf{Z}$ is the number $\varphi(n)$ of integers k in the interval $1 \leq k \leq n$ satisfying $\mathrm{pgcd}(n, k) = 1$. The map $\varphi : \mathbf{Z}_{>0} \to \mathbf{Z}$ is *Euler's function* already mentioned in § 1.1. If $\gcd(a, b) = d$, then a/d and b/d are relatively prime. Hence, the partition of the set of integers in $1 \leq k \leq n$ according to the value of $\gcd(k, n)$ yields:

Lemma 3. *For any positive integer n,*

$$n = \sum_{d|n} \varphi(d).$$

(Compare with (30)).

An *arithmetic function* is a map $f : \mathbf{Z}_{>0} \to \mathbf{Z}$. A *multiplicative function* is an arithmetic function such that $f(mn) = f(m)f(n)$ when m and n are relatively prime. For instance, Euler's φ function is multiplicative: this follows from the ring isomorphim between the ring product $(\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$ and the ring $\mathbf{Z}/mn\mathbf{Z}$ when m and n are relatively prime (*Chinese remainder Theorem*). Also, $\varphi(p^a) = p^{a-1}(p-1)$ for p prime and $a \geq 1$. Hence, the value of $\varphi(n)$, for n written as a product of powers of distinct prime numbers, is

$$\varphi(p_1^{a_1} \cdots p_r^{a_r}) = p_1^{a_1-1}(p_1-1) \cdots p_r^{a_r-1}(p_r-1).$$

Primitive roots modulo a prime number p: there are exactly $\varphi(p-1)$ of them in $(\mathbf{Z}/p\mathbf{Z})^\times$. An element $g \in (\mathbf{Z}/p\mathbf{Z})^\times$ is a primitive root modulo p if and only if

$$g^{(p-1)/q} \not\equiv 1 \bmod p$$

for all prime divisors q of $p-1$.

If a and n are relatively prime integers, the *order of a modulo n* is the order of the class of a in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. In other terms, it is the smallest integer ℓ such that a^ℓ is congruent to 1 modulo n.

Exercise 4. For n a positive integer, check that the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is either 2, 4, p^s or $2p^s$, with p an odd prime and $s \geq 1$.

`Remark:` *For $s \geq 2$, $(\mathbf{Z}/2^s\mathbf{Z})^\times$ is the product of a cyclic group of order 2 by a cyclic group of order 2^{s-2}, hence, for $s \geq 3$ it is not cyclic.*

1.4.2 The ring $\mathbf{Z}[X]$

When F is a field, the ring $F[X]$ of polynomials in one variable over F is an Euclidean domain, hence, a principal domain, and, therefore, a factorial ring. The ring $\mathbf{Z}[X]$ is not an Euclidean ring: one cannot divide X by 2 in $\mathbf{Z}[X]$ for instance. But if A and B are in $\mathbf{Z}[X]$ and B is monic, then both the quotient Q and the remainder R of the Euclidean division in $\mathbf{Q}[X]$ of A by B

$$A = BQ + R$$

are in $\mathbf{Z}[X]$.

The gcd of the coefficients of a non–zero polynomial $f \in \mathbf{Z}[X]$ is called the *content* of f. We denote it by $c(f)$. A non–zero polynomial with content 1 is called *primitive*. Any non–zero polynomial in $\mathbf{Z}[X]$ can be written in a unique way as $f = c(f)g$ with $g \in \mathbf{Z}[X]$ primitive.

For any non–zero polynomial $f \in \mathbf{Q}[X]$, there is a unique positive rational number r such that rf belongs to $\mathbf{Z}[X]$ and is primitive.

Lemma 5 (Gauss's Lemma)**.** *For f and g non–zero polynomials in $\mathbf{Z}[X]$, we have*

$$c(fg) = c(f)c(g).$$

Proof. It suffices to check that the product of two primitive polynomials is primitive. More generally, let p be a prime number and f, g two polynomials whose contents are not divisible by p. We check that the content of fg is not divisible by p.

Recall the surjective morphism of rings (1) $\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X]$,, which is the reduction modulo p. The kernel of Ψ_p is the set of polynomials whose content is divisible by p. The assumption is $\Psi_p(f) \neq 0$ and $\Psi_p(g) \neq 0$. Since p is prime, the ring $\mathbf{F}_p[X]$ has no zero divisor, hence, $\Psi_p(fg) = \Psi_p(f)\Psi_p(g) \neq 0$, which shows that fg is not in the kernel of Ψ_p. □

The ring $\mathbf{Z}$ is an Euclidean domain, hence, a principal domain, and, therefore, a factorial ring. It follows that the ring $\mathbf{Z}[X]$ is factorial. The units of $\mathbf{Z}[X]$ are $\{+1, -1\}$. The irreducible elements in $\mathbf{Z}[X]$ are
– the prime numbers $\{2, 3, 5, 7, 11, \dots\}$,
– the irreducible polynomials in $\mathbf{Q}[X]$ with coefficients in $\mathbf{Z}$ and content 1
– and, of course, the product of one of these elements by -1.

From Gauss's Lemma 5, one deduces that if f and g are two monic polynomials in $\mathbf{Q}[X]$ such that $fg \in \mathbf{Z}[X]$, then f and g are in $\mathbf{Z}[X]$.

A monic polynomial in $\mathbf{Z}[X]$ is a product, in a unique way, of irreducible monic polynomials in $\mathbf{Z}[X]$.

1.4.3 Möbius inversion formula

Let f be a map defined on the set of positive integers with values in an additive group. Define another map g by

$$g(n) = \sum_{d|n} f(d).$$

It is easy to check by induction that f is completely determined by g. Indeed, the formula for $n = 1$ produces $f(1) = g(1)$, and for $n \geq 2$, once $f(d)$ is known for all $d \mid n$ with $d \neq n$, one obtains $f(n)$ from the formula

$$f(n) = g(n) - \sum_{\substack{d|n \\ d\neq n}} f(d).$$

We wish to write this formula in a close form. If p is a prime, the formula becomes $f(p) = g(p) - g(1)$. Next, $f(p^2) = g(p^2) - g(p)$. More generally, for p prime and $m \geq 1$,

$$f(p^m) = g(p^m) - g(p^{m-1}).$$

It is convenient to write this formula as

$$f(p^m) = \sum_{h=0}^{m} \mu(p^{m-h}) g(p^h),$$

where $\mu(1) = 1$, $\mu(p) = -1$, $\mu(p^m) = 0$ for $m \geq 2$. In order to extend this formula for writing $f(n)$ in terms of $g(d)$ for $d \mid n$, one needs to extend the function μ, and it is easily seen by means of the convolution product (see Exercise 6) that the right thing to do is to require that μ be a *multiplicative function*, namely that $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime.

The *Möbius function* μ (see, for instance, [8] § 2.6) is the map from the positive integers to $\{0, 1, -1\}$ defined by the properties $\mu(1) = 1$, $\mu(p) = -1$ for p prime, $\mu(p^m) = 0$ for p prime and $m \geq 2$, and $\mu(ab) = \mu(a)\mu(b)$ if a and b are relatively prime. Hence, $\mu(a) = 0$ if and only if a has a square factor, while for a squarefree number a, which is a product of s distinct primes we have $\mu(a) = (-1)^s$:

$$\mu(p_1 \cdots p_s) = (-1)^s.$$

One of the many variants of the *Möbius inversion formula* states that, for f and g two maps defined on the set of positive integers with values in an additive group, the two following properties are equivalent:
(i) *For any integer* $n \geq 1$,

$$g(n) = \sum_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

For instance, Lemma 3 is equivalent to

$$\varphi(n) = \sum_{d|n} \mu(n/d) d \quad \text{for all } n \geq 1.$$

An equivalent statement of the Möbius inversion formula is the following multiplicative version, which deals with two maps f, g from the positive integers into an abelian multiplicative group. The two following properties are equivalent:
(i) *For any integer* $n \geq 1$,

$$g(n) = \prod_{d|n} f(d).$$

(ii) *For any integer* $n \geq 1$,

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

A third form of the Möbius inversion formula (which we will not use here) deals with two functions F and G from $[1, +\infty)$ to $\mathbf{C}$. The two following properties are equivalent:
(i) *For any real number* $x \geq 1$,

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) *For any real number* $x \geq 1$,

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

As an illustration, take $F(x) = 1$ and $G(x) = [x]$ for all $x \in [1, +\infty)$. Then

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

Exercise 6. Let A be a (commutative) ring and let R denote the set of *arithmetic functions*, namely the set of applications from the positive integers into A. For f and g in R, define the convolution product

$$f \star g(m) = \sum_{ab=m} f(a)g(b).$$

(a) Check that R, with the usual addition and with this convolution product, becomes a commutative ring.
`Hint:`

$$f \star g \star h(m) = \sum_{abc=m} f(a)g(b)h(c).$$

Check that the unity is $\delta \in R$ defined by

$$\delta(a) = \begin{cases} 1 & \text{for } a = 1, \\ 0 & \text{for } a > 1. \end{cases}$$

(b) Check that if f and g are multiplicative, then so is $f \star g$.
(c) Define $\mathbf{1} \in R$ by $\mathbf{1}(x) = 1$ for all $x \geq 1$. Check that μ and $\mathbf{1}$ are inverse each other in R:

$$\mu \star \mathbf{1} = \delta.$$

(d) Check that the formula

$$\mu \star \mathbf{1} \star f = f \quad \text{for all } f \in R$$

is equivalent to Möbius inversion formula.
(e) Define j by $j(n) = n$ and, for $k \geq 0$, $\sigma_k(n) = \sum_{d|n} d^k$. Check

$$\mu \star j = \varphi, \quad j^k \star \mathbf{1} = \sigma_k.$$

2 The theory of finite fields

References:

M. Demazure [2], Chap. 8.
D.S. Dummit & R.M. Foote [3], § 14.3.
S. Lang [5], Chap. 5 § 5.
R. Lidl & H. Niederreiter [6].
V. Shoup [8], Chap. 20.

2.1 Gauss fields

A field with finitely many elements is also called a *Gauss Field*. For instance, given a prime number p, the quotient $\mathbf{Z}/p\mathbf{Z}$ is a Gauss field. Given two fields F and F' with p elements, p prime, there is a unique isomorphism $F \to F'$. Hence, we denote by $\mathbf{F}_p$ the unique field with p elements.

The characteristic of finite field F is a prime number p, hence, its prime field is $\mathbf{F}_p$. Moreover, F is a finite vector space over $\mathbf{F}_p$; if the dimension of this space is s, which means that F is a finite extension of $\mathbf{F}_p$ of degree $[F : \mathbf{F}_p] = s$, then F has p^s elements. Therefore, the number of elements of a finite field is always a power of a prime number p, and this prime number is the characteristic of F.

The multiplicative group $F^\times$ of a field with q elements has order $q-1$, hence, $x^{q-1} = 1$ for all x in $F^\times$, and $x^q = x$ for all x in F. Therefore, $F^\times$ is the set of roots of the polynomial $X^{q-1} - 1$, while F is the set of roots of the polynomial $X^q - X$:

$$X^{q-1} - 1 = \prod_{x \in F^\times} (X - x), \qquad X^q - X = \prod_{x \in F} (X - x). \tag{7}$$

Exercise 8. (a) Let F be a finite field with q elements, where q is odd. Denote by $\mathcal{C}$ the set of non–zero squares in F, which is the image of the endomorphism $x \mapsto x^2$ of the multiplicative group $F^\times$:

$$\mathcal{C} = \{x^2 \ \mid \ x \in F^\times\}.$$

Check

$$X^{(q-1)/2} - 1 = \prod_{x \in \mathcal{C}} (X - x) \quad \text{and} \quad X^{(q-1)/2} + 1 = \prod_{x \in F^\times \setminus \mathcal{C}} (X - x)$$

(b) Let p be an odd prime. For a in $\mathbf{F}_p$, denote by $\left(\frac{a}{p}\right)$ the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a non–zero square in } \mathbf{F}_p \\ -1 & \text{if } a \text{ is not a square in } \mathbf{F}_p. \end{cases}$$

Check

$$X^{(p-1)/2} - 1 = \prod_{a \in \mathbf{F}_p,\, \left(\frac{a}{p}\right) = 1} (X - a)$$

and

$$X^{(p-1)/2} + 1 = \prod_{a \in \mathbf{F}_p,\, \left(\frac{a}{p}\right) = -1} (X - a).$$

Deduce that for a in $\mathbf{F}_p$,

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}.$$

Exercise 9. Prove that in a finite field, any element is a sum of two squares.

Exercise 10. Prove that if F is a finite field with q elements, then the polynomial $X^q - X + 1$ has no root in F. Deduce that F is not algebraically closed.

Proposition 11. *Any finite subgroup of the multiplicative group of a field K is cyclic. If n is the order of G, then G is the set of roots of the polynomial $X^n - 1$ in K.*

Proof. The last part of the statement is easy: any element x of G satisfies $x^n = 1$ by Lagrange's theorem, hence the polynomial $X^n - 1$, which has degree n, has n roots in K, namely the elements in G. Since K is a field, we deduce

$$X^n - 1 = \prod_{x \in G} (X - x),$$

which means that G is the set of roots of the polynomial $X^n - 1$ in K

Let e be the exponent go G. By Lagrange's theorem, e divides n. Any x in G is a root of the polynomial $X^e - 1$. Since G has order n, we get n roots in the field K of this polynomial $X^e - 1$ of degree $e \leq n$. Hence $e = n$. We conclude by using the fact that there exists in G at least one element of order e, hence, G is cyclic. □

Second proof of Proposition 11. The following alternative proof of Proposition 11 does not use the exponent. Let K be a field and G a finite subgroup of $K^\times$ of order n. For any divisor d of n, denote by $N_G(d)$ the number of elements in G of order d. By Lagrange's Theorem

$$n = \sum_{d|n} N_G(d). \tag{12}$$

Let d be a divisor of n. If $N_G(d) > 0$, that is, if there exists an element ζ in G of order d, then the cyclic subgroup of G generated by ζ has order d, hence it has $\varphi(d)$ generators. These $\varphi(d)$ elements in K are roots of Φ_d and, therefore, they are all the roots of Φ_d in K. It follows that there are exactly $\varphi(d)$ elements of order d in G. This proves that $N_G(d)$ is either 0 or $\varphi(d)$. From (12) and Lemma 3, we deduce

$$n = \sum_{d|n} N_G(d) \leq \sum_{d|n} \varphi(d) = n,$$

hence, $N_G(d) = \varphi(d)$ for all $d|n$. In particular $N_G(n) > 0$, which means that G is cyclic. □

Programs giving a generator of the cyclic group $\mathbf{F}_q^\times$, also called a *primitive root* or a *primitive element* in $\mathbf{F}_q$, are available online[1].

Exercise 13. Let F be a finite field, q the number of its elements, k a positive integer. Denote by $\mathcal{C}_k$ the image of the endomorphism $x \mapsto x^k$ of the multiplicative group $F^\times$:

$$\mathcal{C}_k = \{x^k \mid x \in F^\times\}.$$

How many elements are there in $\mathcal{C}_k$?

[1] One of them (in French) is
`http://jean-paul.davalan.pagesperso-orange.fr/mots/comb/gfields/index.html`
Computation on finite fields can be done also with
`http://wims.unice.fr/~wims/`

Recall that when $F = \mathbf{F}_p$, a rational integer a is called a primitive root modulo p if a is not divisible by p and if the class of a modulo p is a generator of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times$. More generally, when $\mathbf{F}_q$ is a finite field with q elements, a nonzero element α in $\mathbf{F}_q$ is a generator of the cyclic group $\mathbf{F}_q^\times$ if and only if α is a primitive $(q-1)$th root of unity.

The theorem of the primitive element for finite fields is:

Proposition 14. *Let F be a finite field and K a finite extension of F. Then there exist $\alpha \in K$ such that $K = F(\alpha)$.*

Proof. Let $q = p^s$ be the number of elements in K, where p is the characteristic of F and K; the multiplicative group $K^\times$ is cyclic (Proposition 11); let α be a generator. Then

$$K = \left\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\right\} = \mathbf{F}_p(\alpha),$$

and, therefore, $K = F(\alpha)$.

□

Hence the field K is isomorphic to the quotient $\mathbf{F}_p[X]/(P)$ where $P \in \mathbf{F}_p[X]$ is any irreducible polynomial over $\mathbf{F}_p$ of degree s.

Lemma 15. *Let K be a field of characteristic p. For x and y in K, we have $(x+y)^p = x^p + y^p$.*

Proof. When p is a prime number and n an integer in the range $1 \leq n < p$, the binomial coefficient

$$\binom{p}{n} = \frac{p!}{n!(p-n)!}$$

is divisible by p. □

We now prove that for any prime number p and any integer $s \geq 1$, there exists a finite field with p^s elements.

Theorem 16. *Let p be a prime number and s a positive integer. Set $q = p^s$. Then there exists a field with q elements. Two finite fields with the same number of elements are isomorphic. If Ω is an algebraically closed field of characteristic p, then Ω contains one and only one subfield with q elements.*

Proof. Let F be a splitting field over $\mathbf{F}_p$ of the polynomial $X^q - X$. Then F is the set of roots of this polynomial, hence, has q elements.

If F' is a field with q elements, then F' is the set of roots of the polynomial $X^q - X$, hence, F' is the splitting field of this polynomial over its prime field, and, therefore, is isomorphic to F.

If Ω is an algebraically closed field of characteristic p, then the unique subfield of Ω with q elements is the set of roots of the polynomial $X^q - X$.

□

According to (7), if $\mathbf{F}_q$ is a finite field with q elements and F an extension of $\mathbf{F}_q$, then for $a \in F$, the relation $a^q = a$ holds if and only if $a \in \mathbf{F}_q$. We will use the following more general fact:

Lemma 17. *Let $\mathbf{F}_q$ be a finite field with q elements, F an extension of $\mathbf{F}_q$ and $f \in F[X]$ a polynomial with coefficients in F. Then f belongs to $\mathbf{F}_q[X]$ if and only if $f(X^q) = f(X)^q$.*

Proof. Since q is a power of the characteristic p of F, if we write

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

then, by Lemma 15,

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}$$

and by induction

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}.$$

Therefore, $f(X)^q = f(X^q)$ if and only if $a_i^q = a_i$ for all $i = 0, 1, \ldots, n$.

□

From Lemma 15, we deduce:

Proposition 18. *Let F be a field of characteristic p.*
(a) The map

$$\begin{array}{rccc} \mathrm{Frob}_p : & F & \to & F \\ & x & \mapsto & x^p \end{array}$$

is an endomorphism of F.
(b) If F is finite, or if F is algebraically closed, then Frob_p is surjective, hence is an automorphism of the field F.

`Remark`. An example of a field of characteristic p for which Frob_p is not surjective is the field $\mathbf{F}_p(X)$ of rational fractions in one variable over the prime field $\mathbf{F}_p$.

Proof. Indeed, this map is a morphism of fields since, by Lemma 15, for x and y in F,

$$\mathrm{Frob}_p(x + y) = \mathrm{Frob}_p(x) + \mathrm{Frob}_p(y)$$

and

$$\mathrm{Frob}_p(xy) = \mathrm{Frob}_p(x)\mathrm{Frob}_p(y).$$

It is injective since it is a morphism of fields. If F is finite, it is surjective because it is injective. If F is algebraically closed, any element in F is a p–th power. □

This automorphism of F is called the *Frobenius* of F over $\mathbf{F}_p$. It extends to an automorphism of the algebraic closure of F.

If s is a non–negative integer, we denote by Frob_p^s or by Frob_{p^s} the iterated automorphism

$$\mathrm{Frob}_p^0 = 1, \quad \mathrm{Frob}_{p^s} = \mathrm{Frob}_{p^{s-1}} \circ \mathrm{Frob}_p \qquad (s \geq 1),$$

so that, for $x \in F$,

$$\mathrm{Frob}_p^0(x) = x,\ \mathrm{Frob}_p(x) = x^p,\ \mathrm{Frob}_{p^2}(x) = x^{p^2}, \ldots,\ \mathrm{Frob}_{p^s}(x) = x^{p^s} \quad (s \geq 0).$$

If F has p^s elements, then the automorphism $\mathrm{Frob}_p^s = \mathrm{Frob}_{p^s}$ of F is the identity.

If F is a finite field with q elements and K a finite extension of F, then Frob_q is a F–automorphism of K called the *Frobenius of K over F*.

Let F be a finite field of characteristic p with $q = p^r$ elements. According to Proposition 11, the multiplicative group $F^\times$ of F is cyclic of order $q-1$. Let α be a generator of $F^\times$, that means an element of order $q-1$. For $1 \leq \ell < r$, we have $1 \leq p^\ell - 1 < p^r - 1 = q - 1$, hence, $\alpha^{p^\ell - 1} \neq 1$ and $\mathrm{Frob}_p^\ell(\alpha) \neq \alpha$. Since Frob_p^r is the identity on F, it follows that Frob_p has order r in the group of automorphisms of F.

Recall that a finite extension L/K is called *a Galois extension* if the group G of K–automorphisms of L has order $[L : K]$, and in this case the group G is the Galois group of the extension, denoted by $\mathrm{Gal}(L/K)$. It follows that the extension $F/\mathbf{F}_p$ is Galois, with Galois group $\mathrm{Gal}(F/\mathbf{F}_p) = \mathrm{Aut}(F)$ the cyclic group of order s generated by Frob_p.

We extend this result to the more general case where the ground field $\mathbf{F}_p$ is replaced by any finite field.

Theorem 19. *[Galois theory for finite fields]*

Let F be a finite field with q elements and K a finite extension of F of degree s. Then the extension K/F is Galois with Galois group $\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K)$ *the cyclic group generated by the Frobenius* Frob_q. *Define* $G = \mathrm{Gal}(K/F)$.

$$\begin{array}{rc} & K \\ s/d & | \\ & E \\ d & | \\ & F \end{array} \Big) s$$

There is a bijection between
(i) the divisors d of s.
(ii) the subfields E of K containing F
(iii) the subgroups H of G.

• *If E is a subfield of K containing F, then the degree $d = [K : E]$ of E over K divides s, the number of elements in E is q^d, the extension K/F is Galois with Galois group the unique subgroup H of G of order d, which is the subgroup generated by* Frob_{q^d}*; furthermore, H is the subgroup of G which consists of the elements $\sigma \in G$ such that $\sigma(x) = x$ for all $x \in E$.*

• *Conversely, if d divides s, then K has a unique subfield E with q^d elements, which is the fixed field by* Frob_{q^d}*:*

$$E = \{\alpha \in K \ \mid \ \mathrm{Frob}_{q^d}(\alpha) = \alpha\},$$

this field E contains F, and the Galois group of K over E is the unique subgroup H of G of order d.

Proof. Since G is cyclic generated by Frob_q, there is a bijection between the divisors d of s and the subgroups H of G: for $d|s$, the unique subgroup of G of order s/d (which means of index d) is the cyclic subgroup generated by Frob_{q^d}. The fixed field of H, which is by definition the set of x in K satisfying $\sigma(x) = x$ for all $\sigma \in H$, is the fixed field of Frob_{q^d}, hence it is the unique subfield of E with q^d elements; the degree of K over E is therefore d. If E is the subfield of K with q^d elements, then the Galois group of K/E is the cyclic group generated by Frob_{q^d}. □

Under the hypotheses of Theorem 19, the Galois group of E over F is the quotient $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Exercise 20.
(a) Let F be a field, m and n two positive integers, a and b two integers ≥ 2. Prove that the following conditions are equivalent.
(i) n divides m.
(ii) In $F[X]$, the polynomial $X^n - 1$ divides $X^m - 1$.
(iii) $a^n - 1$ divides $a^m - 1$.
(ii') In $F[X]$, the polynomial $X^{a^n} - X$ divides $X^{a^m} - X$.
(iii') $b^{a^n} - b$ divides $b^{a^m} - b$.
(b) Let m, n and a be positive integers with $a \geq 2$. Check

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1.$$

Fix an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. For each $s \geq 1$, denote by $\mathbf{F}_{p^s}$ the unique subfield of Ω with p^s elements. For n and m positive integers, we have the following equivalence:

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divides } m. \tag{21}$$

If these conditions are satisfied, then $\mathbf{F}_{p^m}/\mathbf{F}_{p^n}$ is cyclic, with Galois group of order m/n generated by Frob_{p^n}.

Let $F \subset \overline{\mathbf{F}}_p$ be a finite field of characteristic p with q elements, and let x be an element in $\overline{\mathbf{F}}_p$. The conjugates of x over F are the roots in $\overline{\mathbf{F}}_p$ of the irreducible polynomial of x over F, and these are exactly the images of x by the iterated Frobenius Frob_{q^i}, $i \geq 0$.

Two fields with p^s elements are isomorphic (cf. Theorem 16), but if $s \geq 2$, there is no unicity of such an isomorphic, because the set of automorphisms of $\mathbf{F}_{p^s}$ has more than one element (indeed, it has s elements).

`Remarks`.

- The additive group $(F, +)$ of a finite field F with q elements is cyclic if and only if q is a prime number.

- The multiplicative group $(F^\times, \times)$ of a finite field F with q elements is cyclic, hence, is isomorphic to the additive group $\mathbf{Z}/(q-1)\mathbf{Z}$.

- A finite field F with q elements is isomorphic to the ring $\mathbf{Z}/q\mathbf{Z}$ if and only if q is a prime number (which is equivalent to saying that $\mathbf{Z}/q\mathbf{Z}$ has no zero divisor).

Example 22 (`Simplest example of a finite field which is not a prime field).` A field F with 4 elements has two elements besides 0 and 1. These two elements play exactly the same role: the map which permutes them and sends 0 to 0 and 1 to 1 is an automorphism of F: this automorphism is nothing else than Frob_2. Select one of these two elements, call it j. Then j is a generator of the multiplicative group $F^\times$, which means that $F^\times = \{1, j, j^2\}$ and $F = \{0, 1, j, j^2\}$.

Here are the addition and multiplication tables of this field F:

$(F,+)$	0	1	j	j^2
0	0	1	j	j^2
1	1	0	j^2	j
j	j	j^2	0	1
j^2	j^2	j	1	0

$(F,\times)$	0	1	j	j^2
0	0	0	0	0
1	0	1	j	j^2
j	0	j	j^2	1
j^2	0	j^2	1	j

There are 4 polynomials of degree 2 over $\mathbf{F}_2$, three of them split in $\mathbf{F}_2$, namely X^2, $X^2+1 = (X+1)^2$ and $X^2+X = X(X+1)$, and just one which is irreducible, $X^2 + X + 1$, the roots of which are the elements of F other than 0 and 1.

Example 23 (`The field` $\mathbf{F}_5$`).` .

We could write $\mathbf{F}_5 = \{0, 1, -1, i, -i\}$ with i and $-i$ the two roots of $X^2 + 1$, one of them is 2, the other is 3. Notice that there is no automorphism of $\mathbf{F}_5$ mapping i to $-i$.

Exercise 24. Check the following isomorphisms, and give a generator of the multiplicative group of non–zero elements in the field.
(a) $\mathbf{F}_4 = \mathbf{F}_2[X]/(X^2 + X + 1)$.
(b) $\mathbf{F}_8 = \mathbf{F}_2[X]/(X^3 + X + 1)$.
(c) $\mathbf{F}_{16} = \mathbf{F}_2[X]/(X^4 + X + 1)$.
(d) $\mathbf{F}_{16} = \mathbf{F}_2[X, Y]/(Y^2 + Y + 1, X^2 + X + Y)$.

Exercise 25. (a) Give the list of all irreducible polynomials of degree ≤ 5 over $\mathbf{F}_2$.
(b) Give the list of all monic irreducible polynomials of degree ≤ 2 over $\mathbf{F}_4$.

Recall (Theorem 19) that any finite extension of a finite field is Galois. Hence, in a finite field F, any irreducible polynomial is separable: *finite fields are perfect.*

Theorem 26 (Normal basis theorem)**.** *Given a finite extension $L \supset K$ of finite fields, there exists an element α in $L^\times$ such that the conjugates of α over K form a basis of the vector space L over K.*
With such a basis, the Frobenius map Frob_q*, where q is the number of elements in K, becomes a shift operator on the coordinates.*

`Remark`. The normal basis Theorem holds for any finite Galois extension L/K: given any finite Galois extension L/K, there exists $\alpha \in L$ such that the conjugates of α give a basis of the K vector space L. We first give a proof of this result when K is infinite, and then a proof for a cyclic extension L/K. The second proof will give the result for finite fields.

Let $G = \mathrm{Gal}(L/K)$. The conjugates of α over K are the elements $\sigma(\alpha)$. Consider a linear relation with coefficients in K among such numbers, for an arbitrary $\alpha \in L$:

$$\sum_{\sigma \in G} a_\sigma \sigma(\alpha) = 0.$$

For each $\tau \in G$, we also have

$$\sum_{\sigma \in G} a_\sigma \tau^{-1}\sigma(\alpha) = 0.$$

Hence, for $\alpha \in L$; a necessary and sufficient condition for the conjugates of α to give a basis of L over K is

$$\det\big(\tau^{-1}\sigma(\alpha)\big)_{\tau,\sigma \in G} \neq 0.$$

Since L/K is a finite separable extension, there exists an element β in L such that $L = K(\beta)$ (*theorem of the primitive element*). Let f be the irreducible polynomial of β over K:

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\beta)).$$

For $\sigma \in G$, define $g^\sigma(X) \in L[X]$ by

$$g^\sigma(X) = \frac{f(X)}{X - \sigma(\beta)} = \prod_{\tau \in G \setminus \{\sigma\}} (X - \tau(\beta)).$$

We have $g^\sigma(\beta) \neq 0$ for $\sigma = 1$ and $g^\sigma(\beta) = 0$ for $\sigma \neq 1$, hence the determinant

$$\mathrm{d}(X) = \det\big(g^{\tau^{-1}\sigma}(X)\big)_{\tau,\sigma \in G}$$

does not vanish at β; this shows that $\mathrm{d}(X)$ is not the zero polynomial

Assume now that the field K is infinite: hence there exists $\gamma \in L$ such that $\mathrm{d}(\gamma) \neq 0$. Set

$$\alpha = \frac{f(\gamma)}{\gamma - \beta}.$$

Then one checks that α and its conjugates give a basis of L over K.

However this argument does not work for a finite field, which is the case we are interested in. In this case a different argument is used, which works more generally for a cyclic extension.

Proof of Theorem 26.
Let σ be a generator of G. The elements of G are distinct characters of $L^\times$, namely homomorphisms of multiplicative groups $L^\times \to L^\times$, and therefore they are linearly independent by Dedekind Theorem (*theorem of linear independence of characters*). We now consider σ as an endomorphism of the K–vector space L: since $1, \sigma, \ldots, \sigma^{d-1}$ are linearly independent over K, with $d = [L : K]$, the minimal polynomial of the endomorphism σ is $X^d - 1$, which is also the characteristic polynomial of this endomorphism. It follows that there is a cyclic vector, which is an element α in L solution of our problem.

For such a basis $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$, an element γ in L has coordinates $a_0, a_1, \ldots, a_{d-1}$ with

$$\gamma = a_0\alpha + a_1\alpha^q + a_2\alpha^{q^2} + \cdots + a_{d-1}\alpha^{q^{d-1}},$$

and the image of γ under the Frobenius map Frob_q is

$$\gamma^q = a_{d-1} + a_0\alpha^q + a_1\alpha^{q^2} + \cdots + a_{d-2}\alpha^{q^{d-1}},$$

the coordinates of which are $a_{d-1}, a_0, a_1, \ldots, a_{d-2}$. Hence the Frobenius is a shift operator on the coordinates.

□

Exercise 27.
a) Let G be a group, N be a normal subgroup of finite index in G and H a subgroup of G. Show that the index of $H \cap N$ in H is finite and divides the index of N in G. Deduce that if $H \cap N = \{1\}$, then H is finite and its order divides the index of N in G.
(b) Let L/K be a finite abelian extension and E_1, E_2 two subfields of L containing K. Assume that the compositum of E_1 and E_2 is L. Show that $[L : E_1]$ divides $[E_2 : K]$.
(c) Let F be a finite field, E an extension of F and α, β two elements in E which are algebraic over F of degree respectively a and b. Assume a and b are relatively prime. Prove that

$$F(\alpha, \beta) = F(\alpha + \beta).$$

One of the main results of the theory of finite fields is the following:

Theorem 28. *Let F be a finite field with q elements, α an element in an algebraic closure of F. There exist integers $\ell \geq 1$ such that $\alpha^{q^\ell} = \alpha$. Denote by n the smallest:*

$$n = \min\{\ell \geq 1 \mid \mathrm{Frob}_q^\ell(\alpha) = \alpha\}.$$

Then the field $F(\alpha)$ has q^n elements, which means that the degree of α over F is n, and the minimal polynomial of α over F is

$$\prod_{\ell=0}^{n-1} \left(X - \mathrm{Frob}_q^\ell(\alpha)\right) = \prod_{\ell=0}^{n-1} \left(X - \alpha^{q^\ell}\right). \tag{29}$$

Proof. Define $s = [F(\alpha) : F]$. By Theorem 19, the extension $F(\alpha)/F$ is Galois with Galois group the cyclic group of order s generated by Frob_q. The conjugates of αover F are the elements $\mathrm{Frob}_q^i(\alpha)$, $0 \leq i \leq s-1$. Hence $s = n$.

□

2.2 Cyclotomic polynomials

Let n be a positive integer. A *n–th root of unity* in a field K is an element of $K^\times$ which satifies $x^n = 1$. This means that it is a torsion element of order dividing n.

A *primitive n–th root of unity* is an element of $K^\times$ of order n: for k in $\mathbf{Z}$, the equality $x^k = 1$ holds if and only if n divides k.

For each positive integer n, the n–th roots of unity in F form a finite subgroup of $F^\times_{\mathrm{tors}}$ having at most n elements. The union of all these subgroups of $F^\times_{\mathrm{tors}}$ is just the torsion group $F^\times_{\mathrm{tors}}$ itself. This group contains 1 and -1, but it could have just one element, like for $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{F}_2(X)$ for instance. The torsion subgroup of $\mathbf{R}^\times$ is $\{\pm 1\}$, the torsion subgroup of $\mathbf{C}^\times$ is infinite.

Let K be a field of finite characteristic p and let n be a positive integer. Write $n = p^r m$ with $r \geq 0$ and $\mathrm{pgcd}(p, m) = 1$. In $K[X]$, we have

$$X^n - 1 = (X^m - 1)^{p^r}.$$

If $x \in K$ satisfies $x^n = 1$, then $x^m = 1$. Therefore, the order of a finite subgroup of $K^\times$ is prime to p.

It also follows that the study of $X^n - 1$ reduces to the study of $X^m - 1$ with m prime to p.

Let n be a positive integer and Ω be an algebraically closed field of characteristic either 0 or a prime number not dividing n. Then the number of primitive n-th roots of unity in Ω is $\varphi(n)$. These $\varphi(n)$ elements are the generators of the unique cyclic subgroup C_n of order n of $\Omega^\times$, which is the group of n-th roots of unity in Ω:

$$C_n = \{x \in \Omega \mid x^n = 1\}.$$

2.2.1 Cyclotomic polynomials over $\mathbf{C}[X]$

The map $\mathbf{C} \to \mathbf{C}^\times$ defined by $z \mapsto e^{2i\pi z/n}$ is a morphism from the additive group $\mathbf{C}$ to the multiplicative group $\mathbf{C}^\times$; this morphism is periodic with period n. Hence, it factors to a morphism from the group $\mathbf{C}/n\mathbf{Z}$ to $\mathbf{C}^\times$: we denote it also by $z \mapsto e^{2i\pi z/n}$. The multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ of the ring $\mathbf{Z}/n\mathbf{Z}$ is the set of classes of integers prime to n. Its order is $\varphi(n)$, where φ is Euler's function.

The $\varphi(n)$ complex numbers

$$e^{2i\pi k/n} \qquad k \in (\mathbf{Z}/n\mathbf{Z})^\times$$

are the primitive roots of unity in $\mathbf{C}$.

For n a positive integer, we define a polynomial $\Phi_n(X) \in \mathbf{C}[X]$ by

$$\Phi_n(X) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - e^{2i\pi k/n}). \tag{30}$$

This polynomial is called the *cyclotomic polynomial of index* n; it is monic and has degree $\varphi(n)$. Since

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{2i\pi k/n}),$$

the partition of the set of roots of unity according to their order shows that

$$X^n - 1 = \prod_{\substack{1 \leq d \leq n \\ d|n}} \Phi_d(X). \tag{31}$$

The degree of $X^n - 1$ is n, and the degree of $\Phi_d(X)$ is $\varphi(d)$, hence, Lemma 3 follows also from (31).

The name **cyclotomy** comes from the Greek and means *divide the circle*. The complex roots of $X^n - 1$ are the vertices of a regular polygon with n sides.

From (31), it follows that an equivalent definition of the polynomials $\Phi_1, \Phi_2, \ldots$ in $\mathbf{Z}[X]$ is by induction on n:

$$\Phi_1(X) = X - 1, \qquad \Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{\substack{d \neq n \\ d|n}} \Phi_d(X)}. \tag{32}$$

This is the most convenient way to compute the cyclotomic polynomials Φ_n for small values of n.

Möbius inversion formula (see the second form in § 1.4.3 with G the multiplicative group $\mathbf{Q}(X)^\times$) yields

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

First examples. One has

$$\Phi_2(X) = \frac{X^2 - 1}{X - 1} = X + 1, \quad \Phi_3(X) = \frac{X^3 - 1}{X - 1} = X^2 + X + 1,$$

and more generally, for p prime

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

The next cyclotomic polynomials are

$$\Phi_4(X) = \frac{X^4 - 1}{X^2 - 1} = X^2 + 1 = \Phi_2(X^2),$$

$$\Phi_6(X) = \frac{X^6 - 1}{(X^3 - 1)(X + 1)} = \frac{X^3 + 1}{X + 1} = X^2 - X + 1 = \Phi_3(-X).$$

Exercise 33.
(a) Let p be a prime number and let $m \geq 1$. Prove

$$\begin{cases} \Phi_m(X^p) = \Phi_{pm}(X) & \text{and} \quad \varphi(pm) = p\varphi(m) & \text{if } p|m, \\ \Phi_m(X^p) = \Phi_{pm}(X)\Phi_m(X) & \text{and} \quad \varphi(pm) = (p-1)\varphi(m) & \text{if } \gcd(p,m) = 1. \end{cases}$$

Deduce

$$\Phi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \Phi_p(X^{p^{r-1}})$$

when p is a prime and $r \geq 1$.
(b) Let n be a positive integer. Prove

$$\varphi(2n) = \begin{cases} \varphi(n) & \text{if } n \text{ is odd}, \\ 2\varphi(n) & \text{if } n \text{ is even}, \end{cases}$$

$$\Phi_{2n}(X) = \begin{cases} -\Phi_1(-X) & \text{if } n = 1, \\ \Phi_n(-X) & \text{if } n \text{ is odd and} \geq 3, \\ \Phi_n(X^2) & \text{if } n \text{ is even}. \end{cases}$$

Deduce, for $\ell \geq 1$ and for m odd ≥ 3,

$$\begin{aligned} &\Phi_{2^\ell}(X) = X^{2^{\ell-1}} + 1 \\ &\Phi_{2^\ell m}(X) = \Phi_m(-X^{2^{\ell-1}}), \\ &\Phi_m(X)\Phi_m(-X) = \Phi_m(X^2). \end{aligned}$$

Theorem 34. *For any positive integer n, the polynomial $\Phi_n(X)$ has its coefficients in $\mathbf{Z}$. Moreover, $\Phi_n(X)$ is irreducible in $\mathbf{Z}[X]$.*

Proof of the first part of Theorem 34. We check $\Phi_n(X) \in \mathbf{Z}[X]$ by induction on n. The results holds for $n = 1$, since $\Phi_1(X) = X - 1$. Assume $\Phi_m(X) \in \mathbf{Z}[X]$ for all $m < n$. From the induction hypothesis, it follows that

$$h(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

is monic with coefficients in $\mathbf{Z}$. We divide $X^n - 1$ by h in $\mathbf{Z}[X]$: let $Q \in \mathbf{Z}[X]$ be the quotient and $R \in \mathbf{Z}[X]$ the remainder:

$$X^n - 1 = h(X)Q(X) + R(X).$$

We also have $X^n - 1 = h(X)\Phi_n(X)$ in $\mathbf{C}[X]$, as shown by (31). From the unicity of the quotient and remainder in the Euclidean division in $\mathbf{C}[X]$, we deduce $Q = \Phi_n$ and $R = 0$, hence, $\Phi_n \in \mathbf{Z}[X]$. □

We now show that Φ_n is irreducible in $\mathbf{Z}[X]$. Since it is monic, its content is 1. It remains to check that it is irreducible in $\mathbf{Q}[X]$.

Here is a proof of the irreducibility of the cyclotomic polynomial in the special case where the index is a prime number p. It rests on Eisenstein's Criterion:

Proposition 35 (Eisenstein criterion)**.** *Let*

$$C(X) = c_0X^d + \cdots + c_d \in \mathbf{Z}[X]$$

and let p be a prime number. Assume C to be product of two polynomials in $\mathbf{Z}[X]$ of positive degrees. Assume also that p divides c_i for $1 \leq i \leq d$ but that p does not divide c_0. Then p^2 divides c_d.

Proof. Let

$$A(X) = a_0X^n + \cdots + a_n \quad \text{and} \quad B(X) = b_0X^m + \cdots + b_m$$

be two polynomials in $\mathbf{Z}[X]$ of degrees m and n such that $C = AB$. Hence, $d = m + n$, $c_0 = a_0b_0$, $c_d = a_nb_m$. We use the morphism (1) of reduction modulo p, namely $\Psi_p : \mathbf{Z}[X] \longrightarrow \mathbf{F}_p[X]$. Write $\tilde{A} = \Psi_p(A)$, $\tilde{B} = \Psi_p(B)$, $\tilde{C} = \Psi_p(C)$,

$$\tilde{A}(X) = \tilde{a}_0X^n + \cdots + \tilde{a}_n, \quad \tilde{B}(X) = \tilde{b}_0X^m + \cdots + \tilde{b}_m$$

and

$$\tilde{C}(X) = \tilde{c}_0X^d + \cdots + \tilde{c}_d.$$

By assumption $\tilde{c}_0 \neq 0$, $\tilde{c}_1 = \cdots = \tilde{c}_d = 0$, hence, $\tilde{C}(X) = \tilde{c}_0X^d = \tilde{A}(X)\tilde{B}(X)$ with $\tilde{c}_0 = \tilde{a}_0\tilde{b}_0 \neq 0$. Now $\tilde{A}$ and $\tilde{B}$ have positive degrees n and m, hence, $\tilde{a}_n = \tilde{b}_m = 0$, which means that p divides a_n and b_m, and, therefore, p^2 divides $c_d = a_nb_m$. □

Proof of the irreducibility of Φ_p over $\mathbf{Z}$ in Theorem 34 for p prime. We set $X - 1 = Y$, so that

$$\Phi_p(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + \binom{p}{1}Y^{p-2} + \cdots + \binom{p}{2}Y + p \in \mathbf{Z}[Y].$$

We observe that p divides all coefficients – but the leading one – of the monic polynomial $\Phi_p(Y + 1)$ and that p^2 does not divide the constant term. We conclude by using Eisenstein's Criterion Proposition 35. □

We now consider the general case.

Proof of the irreducibility of Φ_n over $\mathbf{Z}$ in Theorem 34 for all n. Let $f \in \mathbf{Z}[X]$ be an irreducible factor of Φ_n with a positive leading coefficient and let $g \in \mathbf{Z}[X]$ satisfy $fg = \Phi_n$. Our goal is to prove $f = \Phi_n$ and $g = 1$.

Since Φ_n is monic, the same is true for f and g. Let ζ be a root of f in $\mathbf{C}$ and let p be a prime number which does not divide n. Since ζ^p is a primitive n-th root of unity, it is a zero of Φ_n.

The first and main step of the proof is to check that $f(\zeta^p) = 0$. If ζ^p is not a root of f, then it is a root of g. We assume $g(\zeta^p) = 0$ and we will reach a contradiction.

Since f is irreducible, f is the minimal polynomial of ζ, hence, from $g(\zeta^p) = 0$, we infer that $f(X)$ divides $g(X^p)$. Write $g(X^p) = f(X)h(X)$ and consider the morphism Ψ_p of reduction modulo p already introduced in (1). Denote by F, G, H the images of f, g, h. Recall that $fg = \Phi_n$ in $\mathbf{Z}[X]$, hence, $F(X)G(X)$ divides $X^n - 1$ in $\mathbf{F}_p[X]$. The assumption that p does not divide n implies that $X^n - 1$ has no square factor in $\mathbf{F}_p[X]$.

Let $P \in \mathbf{Z}[X]$ be an irreducible factor of F. From $G(X^p) = F(X)H(X)$, it follows that $P(X)$ divides $G(X^p)$. But $G \in \mathbf{F}_p[X]$, hence (see Lemma 17), $G(X^p) = G(X)^p$ and, therefore, P divides $G(X)$. Now P^2 divides the product FG, which is a contradiction.

We have checked that for any root ζ of f in $\mathbf{C}$ and any prime number p which does not divide n, the number ζ^p is again a root of f. By induction on the number of prime factors of m, it follows that for any integer m with $\gcd(m, n) = 1$ the number ζ^m is a root of f. Now f vanishes at all the primitive n–th roots of unity, hence, $f = \Phi_n$ and $g = 1$.

□

Let n be a positive integer. The *cyclotomic field of level n over* $\mathbf{Q}$ is

$$R_n = \mathbf{Q}\big(\{e^{2i\pi k/n} \mid k \in (\mathbf{Z}/n\mathbf{Z})^\times\}\big) \subset \mathbf{C}.$$

This is the splitting field of Φ_n over $\mathbf{Q}$. If $\zeta \in \mathbf{C}$ is any primitive n–th root of unity, then $R_n = \mathbf{Q}(\zeta)$ and $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ is a basis of R_n as a $\mathbf{Q}$–vector space.

For example we have

$$R_1 = R_2 = \mathbf{Q}, \quad R_3 = R_6 = \mathbf{Q}(j), \quad R_4 = \mathbf{Q}(i),$$

where j is a root of the polynomial $X^2 + X + 1$. It is easy to check that for $n \geq 1$ we have $\varphi(n) = 1$ if and only if $n \in \{1, 2\}$, $\varphi(n) = 2$ if and only if $n \in \{3, 4, 6\}$ and $\varphi(n)$ is even and ≥ 4 for $n \geq 5$ with $n \neq 6$. That $\varphi(n)$, the degree of R_n, tends to infinity with n can be checked in an elementary way.

Exercise 36. *Check*

$$n \leq 2.685\varphi(n)^{1.161}$$

for all $n \geq 1$.

Proposition 37. *There is a canonical isomorphism between* $\mathrm{Gal}(R_n/\mathbf{Q})$ *and the multiplicative group* $(\mathbf{Z}/n\mathbf{Z})^\times$.

Proof. Let ζ_n be a primitive n-th root of unity and let μ_n be the group of n-th roots of unity, which is the subgroup of $\mathbf{C}^\times$ generated by ζ_n. The map $\mathbf{Z} \longrightarrow \mu_n$ which maps m to ζ_n^m is a group homomorphism of kernel $n\mathbf{Z}$. When c is a class modulo n, we denote by ζ^c the image of c under the isomorphism $\mathbf{Z}/n\mathbf{Z} \simeq \mu_n$.

For $\varphi \in \mathrm{Gal}(R_n/\mathbf{Q})$, define $\theta(\varphi) \in (\mathbf{Z}/n\mathbf{Z})^\times$ by

$$\varphi(\zeta_n) = \zeta_n^{\theta(\varphi)}.$$

Then θ is well defined and is a group isomorphism from $\mathrm{Gal}(R_n/\mathbf{Q})$ onto $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Example 38. The element τ in $\mathrm{Gal}(R_n/\mathbf{Q})$ such that $\theta(\tau) = -1$ satisfies $\tau(\zeta_n) = \zeta_n^{-1}$. But ζ_n^{-1} is the complex conjugate of ζ_n, since $|\zeta_n| = 1$. Hence τ is the (restriction to R_n of the) complex conjugation.

Assume $n \geq 3$. The subfield of R_n fixed by the subgroup $\theta^{-1}(\{1, -1\})$ of $\mathrm{Gal}(R_n/\mathbf{Q})$ is the maximal real subfield of R_n:

$$R_n^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = \mathbf{Q}\big(\cos(2\pi/n)\big) = R_n \cap \mathbf{R}$$

with $[R_n : R_n^+] = 2$.

2.2.2 Cyclotomic Polynomials over a finite field

Since Φ_n has coefficients in $\mathbf{Z}$, for any field K, we can view $\Phi_n(X)$ as an element in $K[X]$: in zero characteristic, this is plain since K contains $\mathbf{Q}$; in finite characteristic p, one considers the image of Φ_n under the morphism Ψ_p introduced in (1): we denote again this image by Φ_n.

Proposition 39. *Let K be a field and let n be a positive integer. Assume that K has characteristic either 0 or else a prime number p prime to n. Then the polynomial $\Phi_n(X)$ is separable over K and its roots in K are exactly the primitive n–th roots of unity which belong to K.*

Proof. The derivative of the polynomial $X^n - 1$ is nX^{n-1}. In K, we have $n \neq 0$ since p does not divide n, hence, $X^n - 1$ is separable over K. Since $\Phi_n(X)$ is a factor of $X^n - 1$, it is also separable over K. The roots in K of $X^n - 1$ are precisely the n–th roots of unity contained in K. A n-th root of unity is primitive if and only if it is not a root of Φ_d when $d|n$, $d \neq n$. From (32), this means that it is a root of Φ_n.

□

When $n = p^r m$ with $r \geq 0$ and $m \geq 1$, in characteristic p we have

$$X^n - 1 = (X^m - 1)^{p^r}.$$

Therefore, if p divides n, there is no primitive n–th root of unity in a field of characteristic p.

Exercise 40.
Consider the following polynomials over a field of characteristic p. (a) Prove that for $r \geq 0$ and $m \geq 1$ with $p \not| m$,

$$\Phi_{p^r m}(X) = \Phi_m(X)^{\varphi(p^r)} \quad \text{with} \quad \varphi(p^r) = \begin{cases} 1 & \text{if } r = 0, \\ p^r - p^{r-1} & \text{if } r \geq 1. \end{cases}$$

(b) Deduce that if p divides m, then in characteristic p we have

$$\Phi_{p^r m}(X) = \Phi_m(X)^{p^r}.$$

According to (7), given $q = p^r$, the unique subfield of $\overline{\mathbf{F}}_p$ with q elements is the set $\mathbf{F}_q$ of roots of $X^q - X$ in $\overline{\mathbf{F}}_p$. The set $\{X - x \mid x \in \mathbf{F}_q\}$ is the set of all monic degree 1 polynomials with coefficients in $\mathbf{F}_q$. Hence, (7) is the special case $n = 1$ of the next statement.

Theorem 41. *Let F be a finite field with q elements and let n be a positive integer.The polynomial $X^{q^n} - X$ is the product of all irreducible polynomials in $F[X]$ whose degree divides n. In other terms, for any $n \geq 1$,*

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in E_q(d)} f(X)$$

where $E_q(d)$ is the set all monic irreducible polynomials in $\mathbf{F}_q[X]$ of degree d.

Proof. The derivative of $X^{q^n} - X$ is -1, which has no root, hence, $X^{q^n} - X$ has no multiple factor in characteristic p.

Let $f \in \mathbf{F}_q[X]$ be an irreducible factor of $X^{q^n} - X$ and α be a root of f in $\overline{\mathbf{F}}_p$. The polynomial $X^{q^n} - X$ is a multiple of f, therefore, it vanishes at α, hence, $\alpha^{q^n} = \alpha$ which means $\alpha \in \mathbf{F}_{q^n}$. From the field extensions

$$\mathbf{F}_q \subset \mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^n},$$

we deduce that the degree of α over $\mathbf{F}_q$ divides the degree of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, that is d divides n.

Conversely, let f be an irreducible polynomial in $\mathbf{F}_q[X]$ of degree d where d divides n. Let α be a root of f in $\overline{\mathbf{F}}_p$. Since d divides n, the field $\mathbf{F}_q(\alpha)$ is a subfield of $\mathbf{F}_{q^n}$, hence $\alpha \in \mathbf{F}_{q^n}$ satisfies $\alpha^{q^n} = \alpha$, and therefore f divides $X^{q^n} - X$.

This shows that $X^{q^n} - X$ is a multiple of all irreducible polynomials of degree dividing n.

In the factorial ring $\mathbf{F}_q[X]$, the polynomial $X^{q^n} - X$, having no multiple factor, is the product of the monic irreducible polynomials which divide it. Theorem 41 follows.

□

Denote by $N_q(d)$ the number of elements in $E_q(d)$, that is the number of monic irreducible polynomials of degree d in $\mathbf{F}_q[X]$. Theorem 41 yields, for

$n \geq 1$,

$$q^n = \sum_{d|n} dN_q(d). \tag{42}$$

From Möbius inversion formula (§ 1.4.3), one deduces:

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

For instance, when ℓ is a prime number,

$$N_q(\ell) = \frac{q^\ell - q}{\ell}. \tag{43}$$

Exercise 44. Let F be a finite field with q elements.
(a) Give the values of $N_2(n)$ for $1 \leq n \leq 6$.
(b) Check, for $n \geq 2$,

$$\frac{q^n}{2n} \leq N_q(n) \leq \frac{q^n}{n}.$$

(c) More precisely, check, for $n \geq 2$,

$$\frac{q^n - q^{\lfloor n/2 \rfloor + 1}}{n} < N_q(n) \leq \frac{q^n - q}{n}.$$

(d) Let F be a finite field of characteristic p. Denote by $\mathbf{F}_p$ the prime subfield of F. Check that more than half of the elements α in F satisfy $F = \mathbf{F}_p(\alpha)$.
(e) Check that when p^n tends to infinity, the probability that a polynomial of degree n over $\mathbf{F}_p$ be irreducible in $\mathbf{F}_p[X]$ tends to $1/n$.

Remark. From (c) one deduces that the number $N_q(n)$ of monic irreducible polynomials of degree n over $\mathbf{F}_q$ satisfies

$$N_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

This *Prime Polynomial Theorem* is the analog for polynomials of the *Prime Number Theorem* which asserts that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x},$$

while the Riemann Hypothesis is equivalent to the assertion that the remainder term $\pi(x) - \mathrm{Li}(x)$ is bounded above by $x^{1/2+o(1)}$. This analogy takes into account the fact that x is the number of integers $\leq x$ while q^n is the number of monic polynomials of degree n over $\mathbf{F}_q$.

2.3 Decomposition of cyclotomic polynomials over a finite field

In all this section, we assume that n is not divisible by the characteristic p of $\mathbf{F}_q$.

We apply Theorem 28 to the cyclotomic polynomials.

Theorem 45. *Let $\mathbf{F}_q$ be a finite field with q elements and let n be a positive integer not divisible by the characteristic of $\mathbf{F}_q$. Then the cyclotomic polynomial Φ_n splits in $\mathbf{F}_q[X]$ into a product of irreducible factors, all of the same degree d, where d is the order of q modulo n.*

Recall (see § 1.4.1) that the order of q modulo n is by definition the order of the class of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$ (hence, it is defined if and only if n and q are relatively prime), it is the smallest integer ℓ such that q^ℓ is congruent to 1 modulo n.

Proof. Let ζ be a root of Φ_n in a splitting field K of the polynomial Φ_n over $\mathbf{F}_q$. The order of ζ in the multiplicative group $K^\times$ is n. According to Theorem 28, the degree of ζ over $\mathbf{F}_q$ is he smallest integer $s \geq 1$ such that $\zeta^{q^s-1} = 1$. Hence it is the smallest positive integer s such that n divides $q^s - 1$, and this is the order of the image of q in the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. □

Since an element $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$ if and only if ζ is a root of Φ_n, an equivalent statement to Theorem 45 is the following.

Corollary 46. *If $\zeta \in \overline{\mathbf{F}}_p^\times$ has order n in the multiplicative group $\overline{\mathbf{F}}_p^\times$, then its degree $d = [\mathbf{F}_q(\zeta) : \mathbf{F}_q]$ over $\mathbf{F}_q$ is the order of q modulo n.*

The special case $d = 1$ of corollary 46 produces the next result:

Corollary 47. *The polynomial $\Phi_n(X)$ splits completely in $\mathbf{F}_q[X]$ (into a product of linear polynomials) if and only if $q \equiv 1 \bmod n$.*

This follows from Theorem 45, but it is also plain from Proposition 11 and the fact that the cyclic group $\mathbf{F}_q^\times$ of order $q-1$ contains a subgroup of order n if and only if n divides $q-1$, which is the condition $q \equiv 1 \bmod n$.

The special case $d = \varphi(n)$ of corollary 46 produces the next result:

Corollary 48. *The following conditions are equivalent:*
(i) *The polynomial $\Phi_n(X)$ is irreducible in $\mathbf{F}_q[X]$.*
(ii) *The class of q modulo n has order $\varphi(n)$.*
(iii) *q is a generator of the group $(\mathbf{Z}/n\mathbf{Z})^\times$.*

This can be true only when this multiplicative group is cyclic, which means (see Exercise 4) that n is either

$$2,\ 4,\ \ell^s,\ 2\ell^s$$

where ℓ is an odd prime and $s \geq 1$.

Corollary 49. *Let q be a power of a prime, s a positive integer, and $n = q^s - 1$. Then q has order s modulo n. Hence, Φ_n splits in $\mathbf{F}_q[X]$ into irreducible factors, all of which have degree s.*

Notice that the number of factors in this decomposition is $\varphi(q^s-1)/s$, hence it follows that s divides $\varphi(q^s - 1)$.

Numerical examples

Recall that we fix an algebraic closure $\overline{\mathbf{F}}_p$ of the prime field $\mathbf{F}_p$, and for q a power of p we denote by $\mathbf{F}_q$ the unique subfield of $\overline{\mathbf{F}}_p$ with q elements. Of course, $\overline{\mathbf{F}}_p$ is also an algebraic closure of $\mathbf{F}_q$.

Example 50. The field $\mathbf{F}_4$, quadratic extension of $\mathbf{F}_2$ *(see also example 22).* We consider the quadratic extension $\mathbf{F}_4/\mathbf{F}_2$. There is a unique irreducible polynomial of degree 2 over $\mathbf{F}_2$, which is $\Phi_3 = X^2 + X + 1$. Denote by ζ one of its roots in $\mathbf{F}_4$. The other root is ζ^2 with $\zeta^2 = \zeta + 1$ and

$$\mathbf{F}_4 = \{0,\ 1,\ \zeta,\ \zeta^2\}.$$

If we set $\eta = \zeta^2$, then the two roots of Φ_3 are η and η^2, with $\eta^2 = \eta + 1$ and

$$\mathbf{F}_4 = \{0,\ 1,\ \eta,\ \eta^2\}.$$

There is no way to distinguish these two roots, they play the same role. It is the same situation as with the two roots $\pm i$ of $X^2 + 1$ in $\mathbf{C}$.

Example 51. The field $\mathbf{F}_8$, cubic extension of $\mathbf{F}_2$. We consider the cubic extension $\mathbf{F}_8/\mathbf{F}_2$. There are 6 elements in $\mathbf{F}_8$ which are not in $\mathbf{F}_2$, each of them has degree 3 over $\mathbf{F}_2$, hence, there are two irreducible polynomials of degree 3 in $\mathbf{F}_2[X]$. Indeed, from (43), it follows that $N_2(3) = 2$. The two irreducible factors of Φ_7 are the only irreducible polynomials of degree 3 over $\mathbf{F}_2$:

$$X^8 - X = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

The $6 = \varphi(7)$ elements in $\mathbf{F}_8^\times$ of degree 3 are the six roots of Φ_7, hence, they have order 7. If ζ is any of them, then

$$\mathbf{F}_8 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6\}.$$

Since $[\mathbf{F}_8 : \mathbf{F}_2] = 3$, there are three automorphisms of $\mathbf{F}_8$, namely the identity, Frob_2 and $\mathrm{Frob}_4 = \mathrm{Frob}_2^2$. If ζ is a root of $Q_1(X) = X^3 + X + 1$, then the two other roots are ζ^2 and ζ^4, while the roots of $Q_2(X) = X^3 + X^2 + 1$ are ζ^3, ζ^5 and ζ^6. Notice that $\zeta^6 = \zeta^{-1}$ and $Q_2(X) = X^3 Q_1(1/X)$. Set $\eta = \zeta^{-1}$. Then

$$\mathbf{F}_8 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6\}$$

and

$$Q_1(X) = (X - \zeta)(X - \zeta^2)(X - \zeta^4), \quad Q_2(X) = (X - \eta)(X - \eta^2)(X - \eta^4).$$

For transmission of data, it is not the same to work with ζ or with $\eta = \zeta^{-1}$. For instance, the map $x \mapsto x + 1$ is given by

$$\zeta + 1 = \zeta^3,\ \zeta^2 + 1 = \zeta^6,\ \zeta^3 + 1 = \zeta,\ \zeta^4 + 1 = \zeta^5,\ \zeta^5 + 1 = \zeta^4,\ \zeta^6 + 1 = \zeta^2$$

and by

$$\eta + 1 = \eta^5,\ \eta^2 + 1 = \eta^3,\ \eta^3 + 1 = \eta^2,\ \eta^4 + 1 = \eta^6,\ \eta^5 + 1 = \eta,\ \eta^6 + 1 = \eta^4.$$

Example 52. The field $\mathbf{F}_9$, quadratic extension of $\mathbf{F}_3$. We consider the quadratic extension $\mathbf{F}_9/\mathbf{F}_3$. Over $\mathbf{F}_3$,

$$X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1).$$

In $\mathbf{F}_9^\times$, there are $4 = \varphi(8)$ elements of order 8 (the four roots of Φ_8) which have degree 2 over $\mathbf{F}_3$. There are two elements of order 4, which are the roots of Φ_4; they are also the squares of the elements of order 8 and they have degree 2 over $\mathbf{F}_3$, their square is -1. There is one element of order 2, namely -1, and one of order 1, namely 1. From (43), it follows that $N_3(2) = 3$: the three monic irreducible polynomials of degree 2 over $\mathbf{F}_3$ are Φ_4 and the two irreducible factors of Φ_8.

Since $[\mathbf{F}_9 : \mathbf{F}_3] = 2$, there are two automorphisms of $\mathbf{F}_9$, namely the identity and Frob_3. Let ζ be a root of $X^2 + X - 1$ and let $\eta = \zeta^{-1}$. Then $\eta = \zeta^7$, $\eta^3 = \zeta^5$ and

$$X^2 + X - 1 = (X - \zeta)(X - \zeta^3), \quad X^2 - X - 1 = (X - \eta)(X - \eta^3).$$

We have

$$\mathbf{F}_9 = \{0,\ 1,\ \zeta,\ \zeta^2,\ \zeta^3,\ \zeta^4,\ \zeta^5,\ \zeta^6,\ \zeta^7\}$$

and also

$$\mathbf{F}_9 = \{0,\ 1,\ \eta,\ \eta^2,\ \eta^3,\ \eta^4,\ \eta^5,\ \eta^6,\ \eta^7\}.$$

The element $\zeta^4 = \eta^4 = -1$ is the element of order 2 and degree 1, and the two elements of order 4 (and degree 2), roots of $X^2 + 1$, are $\zeta^2 = \eta^6$ and $\zeta^6 = \eta^2$.

Exercise 53. Check that 3 has order 5 modulo 11 and that

$$X^{11} - 1 = (X-1)(X^5 - X^3 + X^2 - X - 1)(X^5 + X^4 - X^3 + X^2 - 1)$$

is the decomposition of $X^{11} - 1$ into irreducible factors over $\mathbf{F}_3$.
Remark. Compare with § 3.9.2.

Exercise 54. Check that 2 has order 11 modulo 23 and that $X^{23} - 1$ over $\mathbf{F}_2$ is the product of three irreducible polynomials, namely $X - 1$,

$$X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1$$

and

$$X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1.$$

Remark. Compare with § 3.9.1.

Example 55. Assume that q is odd and consider the polynomial $\Phi_4(X) = X^2 + 1$. Corollary 47 implies:

- If $q \equiv 1 \bmod 4$, then $X^2 + 1$ has two roots in $\mathbf{F}_q$.
- If $q \equiv -1 \bmod 4$, then $X^2 + 1$ is irreducible over $\mathbf{F}_q$.

Example 56. Assume again that q is odd and consider the polynomial $\Phi_8(X) = X^4 + 1$.

- If $q \equiv 1 \bmod 8$, then $X^4 + 1$ has four roots in $\mathbf{F}_q$.
- Otherwise $X^4 + 1$ is a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

For instance, Example 52 gives over $\mathbf{F}_3$

$$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1).$$

Using Example 55, one deduces that in the decomposition of $X^8 - 1$ over $\mathbf{F}_q$, there are

8 linear factors if $q \equiv 1 \bmod 8$,
4 linear factors and 2 quadratic factors if $q \equiv 5 \bmod 8$,
2 linear factors and 3 quadratic factors if $q \equiv -1 \bmod 4$.

Exercise 57. Check that the polynomial $X^4 + 1$ is irreducible over $\mathbf{Q}$ but that it is reducible over $\mathbf{F}_p$ for all prime numbers p.

Example 58. The group $(\mathbf{Z}/5\mathbf{Z})^\times$ is cyclic of order 4, there are $\varphi(4) = 2$ generators which are the classes of 2 and 3. Hence,

- If $q \equiv 2$ or $3 \bmod 5$, then Φ_5 is irreducible in $\mathbf{F}_q[X]$,
- If $q \equiv 1 \bmod 5$, then Φ_5 has 4 roots in $\mathbf{F}_q$,
- If $q \equiv -1 \bmod 5$, then Φ_5 splits as a product of two irreducible polynomials of degree 2 in $\mathbf{F}_q[X]$.

Exercise 59. Let $\mathbf{F}_q$ be a finite field with q elements. What are the degrees of the irreducible factors of the cyclotomic polynomial Φ_{15} over $\mathbf{F}_q$? For which values of q is Φ_{15} irreducible over $\mathbf{F}_q$?

Exercise 60. Let p be a prime number, r a positive integer, $q = p^r$. Denote by $\mathbf{F}_{q^2}$ a field with q^2 elements.
(a) Consider the homomorphism of multiplicative groups $\mathbf{F}_{q^2}^\times \longrightarrow \mathbf{F}_{q^2}^\times$ which maps x to x^{q-1}. What is the kernel? What is the image?
(b) Show that there exists $\alpha \in \mathbf{F}_{q^2}$ such that α^{q-1} is not in $\mathbf{F}_q$. Deduce that (α, α^q) is a basis of the $\mathbf{F}_q$–vector space $\mathbf{F}_{q^2}$.

Decomposition of Φ_n into irreducible factors over $\mathbf{F}_q$

As usual, we assume $\gcd(n, q) = 1$. Theorem 45 tells us that Φ_n is product of irreducible polynomials over $\mathbf{F}_q$ all of the same degree d. Denote by G the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^\times$. Then d is the order of q in G. Let H be the subgroup of G generated by q:

$$H = \{1, q, q^2, \ldots, q^{d-1}\}.$$

Let ζ be any root of Φ_n (in an algebraic closure of $\mathbf{F}_q$, or if you prefer in the splitting field of $\Phi_n(X)$ over $\mathbf{F}_q$). Then the conjugates of ζ over $\mathbf{F}_q$ are its images under the iterated Frobenius Frob_q which maps x to x^q. Hence, the minimal polynomial of ζ over $\mathbf{F}_q$ is

$$P_H(X) = \prod_{i=0}^{d-1}(X - \zeta^{q^i}) = \prod_{h\in H}(X - \zeta^h).$$

This is true for any root ζ of Φ_n. Now fix one of them. Then the others are ζ^m where $\gcd(m, n) = 1$. The minimal polynomial of ζ^m is, therefore,

$$\prod_{i=0}^{d-1}(X - \zeta^{mq^i}).$$

This polynomial can be written

$$P_{mH}(X) = \prod_{h\in mH}(X - \zeta^h)$$

where mH is the class $\{mq^i \mid 0 \le i \le d-1\}$ of m modulo H in G. There are $\varphi(n)/d$ classes of G modulo H, and the decomposition of $\Phi_d(X)$ into irreducible factors over $\mathbf{F}_q$ is

$$\Phi_d(X) = \prod_{mH\in G/H} P_{mH}(X).$$

Factors of $X^n - 1$ in $\mathbf{F}_q[X]$

Again we assume $\gcd(n, q) = 1$. We just studied the decomposition over $\mathbf{F}_q$ of the cyclotomic polynomials, and $X^n - 1$ is the product of the $\Phi_d(X)$ for d dividing n. This gives all the information on the decomposition of $X^n - 1$ in $\mathbf{F}_q[X]$. Proposition 61 below follows from these results, but is also easy to prove directly.

Let ζ be a primitive n-th root of unity in an extension F of $\mathbf{F}_q$. Recall that for j in $\mathbf{Z}$, ζ^j depends only on the classe of j modulo n. Hence, ζ^i makes sense when i is an element of $\mathbf{Z}/n\mathbf{Z}$:

$$X^n - 1 = \prod_{i\in\mathbf{Z}/n\mathbf{Z}}(X - \zeta^i).$$

For each subset I of $\mathbf{Z}/n\mathbf{Z}$, define

$$Q_I(X) = \prod_{i \in I} (X - \zeta^i).$$

For I ranging over the 2^n subsets of $\mathbf{Z}/n\mathbf{Z}$, we obtain all the monic divisors of $X^n - 1$ in $F[X]$. Lemma 17 implies that Q_I belongs to $\mathbf{F}_q[X]$ if and only if $Q_I(X^q) = Q_I(X)^q$.

Since q and n are relatively prime, the multiplication by q, which we denote by $[q]$, defines a permutation of the cyclic group $\mathbf{Z}/n\mathbf{Z}$:

$$\begin{array}{ccc} \mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z} \\ \downarrow & & \downarrow \\ \mathbf{Z}/n\mathbf{Z} & \xrightarrow{[q]} & \mathbf{Z}/n\mathbf{Z} \\ x & \longmapsto & qx. \end{array}$$

The condition $Q_I(X^q) = Q_I(X)^q$ is equivalent to saying that $[q](I) = I$, which means that multiplication by q induces a permutation of the elements in I. We will say for brevity that a subset I of $\mathbf{Z}/n\mathbf{Z}$ with this property is *stable under multiplication by q*. Therefore:

Proposition 61. *The map $I \mapsto Q_I$ is a bijective map between the subsets I of $\mathbf{Z}/n\mathbf{Z}$ which are stable under multiplication by q on the one hand, and the monic divisors of $X^n - 1$ in $\mathbf{F}_q[X]$ on the other hand.*

An irreducible factor of $X^n - 1$ over $\mathbf{F}_q$ is a factor Q such that no proper divisor of Q has coefficients in $\mathbf{F}_q$. Hence,

Corollary 62. *Under this bijective map, the irreducible factors of $X^n - 1$ correspond to the minimal subsets I of $\mathbf{Z}/n\mathbf{Z}$ which are stable under multiplication by q.*

Here are some examples:

- For $I = \emptyset$, $Q_\emptyset = 1$.
- For $I = \mathbf{Z}/n\mathbf{Z}$, $Q_{\mathbf{Z}/n\mathbf{Z}} = X^n - 1$.
- For $I = (\mathbf{Z}/n\mathbf{Z})^\times$, $Q_{(\mathbf{Z}/n\mathbf{Z})^\times} = \Phi_n$.
- For $I = \{0\}$, $Q_0(X) = X - 1$.
- If n is even (and q odd, of course), then for $I = \{n/2\}$, $Q_{\{n/2\}}(X) = X + 1$.
- Let d be a divisor of n. There is a unique subgroup C_d of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. This subgroup is generated by the class of n/d, it is the set of $k \in \mathbf{Z}/n\mathbf{Z}$ such that $dk = 0$, it is stable under multiplication by any element prime to n. Then $Q_{C_d}(X) = X^d - 1$.

- Let again d be a divisor of n and let E_d be the set of generators of C_d: this set has $\varphi(d)$ elements which are the elements of order d in the cyclic group $\mathbf{Z}/n\mathbf{Z}$. Again this subset of $\mathbf{Z}/n\mathbf{Z}$ is stable under multiplication by any element prime to n. Then Q_{E_d} is the cyclotomic polynomial Φ_d of degree $\varphi(d)$.

Example 63. The field $\mathbf{F}_{16}$, quartic extension of $\mathbf{F}_2$. Take $n = 15$, $q = 2$. The minimal subsets of $\mathbf{Z}/15\mathbf{Z}$ which are stable under multiplication by 2 modulo 15 are the classes of

$$\{0\},\ \{5, 10\},\ \{3, 6, 9, 12\},\ \{1, 2, 4, 8\},\ \{7, 11, 13, 14\}.$$

We recover the fact that in the decomposition

$$X^{15} - 1 = \Phi_1(X)\Phi_3(X)\Phi_5(X)\Phi_{15}(X)$$

over $\mathbf{F}_2$, the factor Φ_1 is irreducible of degree 1, the factors Φ_3 and Φ_5 are irreducible of degree 2 and 4 respectively, while Φ_{15} splits into two factors of degree 4 (use the fact that 2 has order 2 modulo 3, order 4 modulo 5 and also order 4 modulo 15).

It is easy to find the two factors of Φ_{15} of degree 4 over $\mathbf{F}_2$. There are four polynomials of degree 4 over $\mathbf{F}_2$ without roots in $\mathbf{F}_2$ (the number of monomials with coefficient 1 should be odd, hence should be 3 or 5) and $\Phi_3^2 = X^4 + X^2 + 1$ is reducible; hence, there are three irreducible polynomials of degree 4 over $\mathbf{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad \Phi_5(X) = X^4 + X^3 + X^2 + X + 1.$$

Therefore, in $\mathbf{F}_2[X]$,

$$\Phi_{15}(X) = (X^4 + X^3 + 1)(X^4 + X + 1).$$

We check the result by computing Φ_{15}: we divide $(X^{15} - 1)/(X^5 - 1) = X^{10} + X^5 + 1$ by $\Phi_3(X) = X^2 + X + 1$ and get in $\mathbf{Z}[X]$:

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Let ζ is a primitive 15-th root of unity (that is, a root of Φ_{15}). Then $\zeta^{15} = 1$ is the root of Φ_1, ζ^5 and ζ^{10} are the roots of Φ_3 (these are the primitive cube roots of unity, they belong to $\mathbf{F}_4$), while $\zeta^3, \zeta^6, \zeta^9, \zeta^{12}$ are the roots of Φ_5 (these are the primitive 5-th roots of unity). One of the two irreducible factors of Φ_{15} has the roots $\zeta, \zeta^2, \zeta^4, \zeta^8$, the other has the roots $\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}$. Also, we have

$$\{\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}\} = \{\zeta^{-1}, \zeta^{-2}, \zeta^{-4}, \zeta^{-8}\}.$$

The splitting field over $\mathbf{F}_2$ of any of the three irreducible factors of degree 4 of $X^{15} - 1$ is the field F_{16} with 2^4 elements, but for one of them (namely Φ_5) the 4 roots have order 5 in $F_{16}^\times$, while for the two others the roots have order 15.

Hence, we have checked that in $\mathbf{F}_{16}^\times$, there are

- 1 element of order 1 and degree 1 over $\mathbf{F}_2$, namely $\{1\} \subset \mathbf{F}_2$,
- 2 elements of order 3 and degree 2 over $\mathbf{F}_2$, namely $\{\zeta^5,\ \zeta^{10}\} \subset \mathbf{F}_4$,
- 4 elements of order 5 and degree 4 over $\mathbf{F}_2$, namely $\{\zeta^3,\ \zeta^6,\ \zeta^9,\ \zeta^{12}\}$,
- 8 elements of order 15 and degree 4 over $\mathbf{F}_2$.

Example 64. The field $\mathbf{F}_{27}$, cubic extension of $\mathbf{F}_3$. Let us write, in $\mathbf{F}_3[X]$,

$$X^{27} - X = X(X^{13} - 1)(X^{13} + 1),$$

$$X^{13} + 1 = (X + 1)f_1 f_2 f_3 f_4, \qquad X^{13} - 1 = (X - 1)f_5 f_6 f_7 f_8$$

with f_i of degree 3. The roots of f_1, f_2, f_3, f_4 are the $12 = \varphi(26)$ generators of the cyclic group $\mathbf{F}_{27}^\times = C_{26}$, the roots of f_5, f_6, f_7, f_8 are the $12 = \varphi(13)$ elements of order 13 which generate the unique cyclic subgroup of $\mathbf{F}_{27}^\times$ of order 13, the root of $X + 1$ is the unique element of order 2.

We are going to exhibit the set $\{f_1, \dots, f_8\}$ by looking at the degree 3 irreducible polynomials over $\mathbf{F}_3$. We will first describe the set $\{f_1, \dots, f_4\}$. Then we can take $f_{4+i}(X) = -f_i(-X)$ (replace X^{2j} by $-X^{2j}$ and keep the sign for X^{2j+1}).

In order to get the decomposition of $X^{13} + 1$, we write the table of discrete logarithms for $\mathbf{F}_{27}$. We need a generator. One among 4 solutions is to take a root α of $X^3 - X + 1$.
Exercise: check $\alpha^{13} = -1$.
`Hint.` Check $\alpha^3 = \alpha - 1$, $\alpha^9 = \alpha^3 - 1 = \alpha + 1$, $\alpha^{12} = \alpha^2 - 1$.

Hence the roots of $X^3 - X + 1$ are α, $\alpha^3 = \alpha - 1$ and $\alpha^9 = \alpha + 1$. We deduce that the roots of the reciprocal polynomial $X^3 + X^2 + 1$ are $\alpha^{-1} = \alpha^{19} - \alpha^2 - \alpha - 1$, $\alpha^{-3} = \alpha^{23} = -\alpha - 1$ and $\alpha^{-9} = \alpha^{17} = -\alpha^2 + \alpha$.

We compute the irreducible polynomial of $\alpha^7 = \alpha^2 - \alpha - 1$, which is also the irreducible polynomial of $\alpha^{21} = \alpha^2 + 1$ and of $\alpha^{63} = \alpha^{11} = \alpha^2 + \alpha + 1$, we find $X^3 + X^2 - X + 1$.

The irreducible polynomial of $\alpha^5 = \alpha^{-21} = -\alpha^2 + \alpha + 1$, which is also the irreducible polynomial of $\alpha^{15} = \alpha^{-11} = 2\alpha^2$ and of $\alpha^{45} = \alpha^{19} = \alpha^7 = -\alpha^2 - \alpha - 1$ is the reciprocal polynomial of the previous one, namely $X^3 - X^2 + X + 1$.

Therefore

$$X^{13} + 1 = (X + 1)(X^3 - X + 1)(X^3 - X^2 + 1)(X^3 + X^2 - X + 1)(X^3 - X^2 + X + 1).$$

The roots of $X^3 - X + 1$ are α, α^3, α^9.
The roots of $X^3 - X^2 + 1$ are $\alpha^{-1} = \alpha^{25}$, $\alpha^{-3} = \alpha^{23}$, $\alpha^{-9} = \alpha^{17}$
The roots of $X^3 + X^2 - X + 1$ are α^7, α^{21}, α^{11}
The roots of $X^3 - X^2 + X + 1$ are $\alpha^{-7} = \alpha^{19}$, $\alpha^{-21} = \alpha^5$, $\alpha^{-11} = \alpha^{15}$.
This gives the list of 12 generators of $\mathbf{F}_{27}^\times$.

The twelve elements of order 13 in $\mathbf{F}_{27}^\times$ are the roots of $(X^{13} - 1)/(X - 1)$, where

$$X^{13} - 1 = (X - 1)(X^3 - X - 1)(X^3 - X^2 - 1)(X^3 - X^2 - X - 1)(X^3 + X^2 + X - 1).$$

Exercise: give the list of the three roots of each of the four factors of $(X^{13}-1)/(X-1)$ over $\mathbf{F}_3$.
`Hint`: consider the change of variable $x \mapsto -x$ using $-1 = \alpha^{13}$.

Exercise 65. Let $\mathbf{F}_q$ be a finite field with q elements of characteristic p. Show that the following conditions are equivalent.
(i) Any element α in $\mathbf{F}_q$ such that $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ is a generator of the cyclic group $\mathbf{F}_q^\times$.
(ii) The number $q-1$ is a prime number.

2.4 Trace and Norm

Let F be a finite field with q elements and let E be a finite extension of degree s of F. For $\alpha \in E$, the *norm of α from E to F* is the product of the conjugates of α over F, while the *trace of α from E to F* is the sum of the conjugates:

$$\mathrm{N}_{E/F}(\alpha) = \prod_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \alpha^{(q^s-1)/(q-1)}, \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}.$$

For $\alpha \in F$, we have $\mathrm{N}_{E/F}(\alpha) = \alpha^s$ and $\mathrm{Tr}_{E/F}(\alpha) = s\alpha$. The norm $\mathrm{N}_{E/F}$ induces a surjective morphism from $E^\times$ onto $F^\times$. The trace $\mathrm{Tr}_{E/F}$ is a F–linear surjective map from E onto F, the kernel of which is the set of roots of the polynomial $X + X^q + \cdots + X^{q^{s-1}}$.

Exercise 66. (a) Let F be a finite field, E a finite extension of F and α a generator of the cyclic group $E^\times$. Check that $\mathrm{N}_{E/F}(\alpha)$ is a generator of the cyclic group $F^\times$.
(b) Deduce that the norm $\mathrm{N}_{E/F}$ induces a surjective morphism from $E^\times$ onto $F^\times$.
(c) Given extensions of finite fields $K \subset F \subset E$, check $\mathrm{N}_{E/K} = \mathrm{N}_{E/F} \circ \mathrm{N}_{F/K}$.
(d) For $x \in F$, define

$$\left(\frac{a}{F}\right) = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \text{ is a non–zero square in } F \\ -1 & \text{if } a \text{ is not a square in } F. \end{cases}$$

Hence Legendre symbol (Exercise 8) is

$$\left(\frac{a}{p}\right) = \left(\frac{\alpha}{\mathbf{F}_p}\right)$$

for $a \in \mathbf{Z}$ and $\alpha = a \pmod p \in \mathbf{F}_p$. Check that if F has q elements with q odd, then, for $a \in F$,

$$\left(\frac{a}{F}\right) = a^{(q-1)/2}.$$

Deduce, for $a \in E$,

$$\left(\frac{a}{E}\right) = \left(\frac{\mathrm{N}_{E/F}(a)}{F}\right).$$

Exercise 67. The field $\mathbf{F}_{16}$, quadratic extension of $\mathbf{F}_4$.

Write $\mathbf{F}_4 = \mathbf{F}_2(j)$ with j root of $X^2 + X + 1$.
(1) List the irreducible polynomials of degree 2 over $\mathbf{F}_4$.
(2) Decompose the 6 irreducible polynomials of $\mathbf{F}_2$ of degree 4 into irreducible factors of degree 2 over $\mathbf{F}_2$.
(Explain why it should be so)
(3) Select a generator of $\mathbf{F}_{16}^\times$ and an irreducible polynomial of degree 2 over $\mathbf{F}_4$ of which α is a root in $\mathbf{F}_{16}$. Write the discrete logarithm table of $\mathbf{F}_{16}^\times$ with basis α. For each of the 15 elements α^k with $0 \leq k \leq 14$, tell which one is the irreducible polynomial of α^k.

Exercise 68. Let $\mathbf{F}_q$ be a finite field of odd characteristic p with $q = p^r$ elements.
(a) Check -1 is a square if and only if $q \equiv 1 \mod 4$.
(b) Assume $p \equiv -1 \mod 4$. Let i be a root of $X^2 + 1$ in $\mathbf{F}_{p^2}$. For a and b in $\mathbf{F}_p$, check

$$(a + ib)^p = a - ib.$$

(Automorphisms of $\mathbf{F}_{p^2}$).
(c) Let p be a Mersenne prime, $p = 2^\ell - 1$ with ℓ prime. Check that for a and b in $\mathbf{F}_p$, $a + ib$ is a generator of the cyclic group $\mathbf{F}_{p^2}^\times$ if and only if $a^2 + b^2$ is a generator of the cyclic group $\mathbf{F}_p^\times$.

2.5 Infinite Galois theory

Let p be a prime number. For each pair (n, m) of positive integers such that n divides m, there exists a field homomorphism from $\mathbf{F}_{p^n}$ into $\mathbf{F}_{p^m}$. Such a morphism is not unique if $n < m$: if we compose it with the Frobenius over $\mathbf{F}_p$, we get another one. For each $n|m$, we choose one of them, say $\iota_{n,m}$, which allow us to consider $\mathbf{F}_{p^n}$ as a subfield of $\mathbf{F}_{p^m}$.Then one checks that the union of the increasing family of fields $\mathbf{F}_{p^{n!}}$ is an algebraic closure of $\mathbf{F}_p$.

Let $\overline{\mathbf{F}}_p$ be an algebraic closure of $\mathbf{F}_p$. The extension $\overline{\mathbf{F}}_p/\mathbf{F}_p$ is algebraic, infinite, normal and separable: it is an *infinite Galois extension*. Its *Galois group* $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ is the group of automorphisms of $\mathbf{F}_p$. It is the projective limit of the Galois groups of the finite extensions of $\mathbf{F}_p$ contained in $\overline{\mathbf{F}}_p/\mathbf{F}_p$:

$$\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) = \varprojlim_{[L:\mathbf{F}_p]<\infty} \mathrm{Gal}(L/\mathbf{F}_p).$$

This group $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ is

$$\hat{\mathbf{Z}} := \varprojlim_{n\to\infty} \mathbf{Z}/n\mathbf{Z}.$$

The projective limite is the set of $(a_n)_{n\geq 1}$ in the Cartesian product $\prod_{n\geq 1} \mathbf{Z}/n\mathbf{Z}$ which satisfy $s_{nm}(a_n) = a_m$ for all pairs of positive integers (n, m) where m divides n, where

$$s_{n,m} : \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z}$$

lis the canonical surjective morphism.

We also have

$$\hat{\mathbf{Z}} := \prod_p \mathbf{Z}_p \quad \text{avec} \quad \mathbf{Z}_p = \varprojlim_{r \to \infty} \mathbf{Z}/p^r\mathbf{Z}.$$

See, for instance, [3] exercise 19 p. 635. and [4] Appendice p. 288.

3 Error correcting codes

From `http://en.wikipedia.org/wiki/Coding_theory`

> *Coding theory is an approach to various science disciplines – such as information theory, electrical engineering, digital communication, mathematics, and computer science – which helps design efficient and reliable data transmission methods so that redundancy can be removed and errors corrected.*
>
> *Channel encoding adds extra data bits to make the transmission of data more robust to disturbances present on the transmission channel.*

Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver. *Error correction* is the additional ability to reconstruct the original, error–free data.

3.1 Some historical dates

Among important dates are the following

• 1949: Marcel Golay (specialist of radars): produced two remarkably efficient codes.

• 1950: Richard W. Hamming, *Error detecting and error correcting codes*, The Bell System Technical Journal **26** (April 1950), N° 2, 147–160.

• 1955: Convolutional codes.

• 1959: Bose Chaudhuri Hocquenghem codes (BCH codes).

• 1960: Reed Solomon codes.

• 1963 John Leech uses Golay's ideas for sphere packing in dimension 24 - classification of finite simple groups

• 1971: no other perfect code than the two found by Golay.

• 1970: Goppa codes.

• 1981: Algebraic geometry codes.

3.2 Hamming distance

The *Hamming distance* on the set $\mathbf{F}_q^n$ is

$$d(\underline{x},\underline{y}) = \#\{i\ ; 1 \leq i \leq n,\ x_i \neq y_i\}$$

for $\underline{x} = (x_1, \ldots, x_n)$ and $\underline{y} = (y_1, \ldots, y_n)$. It satisfies, as it should with the name *distance* (see, for instance, [1], Prop. 10.D),

$$d(\underline{x},\underline{y}) = 0 \Longleftrightarrow \underline{x} = \underline{y}$$

and

$$d(\underline{y},\underline{x}) = d(\underline{x},\underline{y})$$

for $\underline{x}$ and $\underline{y}$ in $\mathbf{F}_q^n$, as well as the triangle inequality for $\underline{x}$, $\underline{y}$ and $\underline{z}$ in $\mathbf{F}_q^n$,

$$d(\underline{x},\underline{z}) \leq d(\underline{x},\underline{y}) + d(\underline{y},\underline{z}).$$

We define the *minimum distance* $d(\mathcal{C})$ of a code $\mathcal{C} \subset \mathbf{F}_q^n$ by

$$d(\mathcal{C}) = \min\{d(\underline{x},\underline{y})\ ;\ \underline{x},\underline{y} \in \mathcal{C},\ \underline{x} \neq \underline{y}\}.$$

The *Hamming weight* $w(\underline{x})$ of an element of $\mathbf{F}_q^n$ is its Hamming distance with 0: for $\underline{x} = (x_1, \ldots, x_n)$:

$$w(\underline{x}) = \#\{i\ ;\ 1 \leq i \leq n,\ x_i \neq 0\}.$$

Hence, for $\underline{x}$ and $\underline{y}$ in $\mathbf{F}_q^n$,

$$d(\underline{x},\underline{y}) = w(\underline{x} - \underline{y}).$$

For t a non–negative integer, the *Hamming ball* $B(\underline{c},t)$ of center $\underline{c} \in \mathbf{F}_q^n$ and radius t is the set of elements of $\mathbf{F}_q^n$ having Hamming distance to $\underline{c}$ at most t:

$$B(\underline{c},t) = \{\underline{x} \in \mathbf{F}_q^n\ ;\ d(\underline{x},\underline{c}) \leq t\}.$$

The number of elements in $B(\underline{c},t)$ is 1 for $t = 0$, it is $1 + n(q-1)$ for $t = 1$, and more generally

$$\#B(\underline{c},t) = 1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \qquad \text{for } t \geq 0. \tag{69}$$

As usual, $\binom{a}{b}$ is defined as 0 when $a < b$. For $t \geq n$ the formula (69) reduces to $\#B(\underline{c},n) = q^n$.

3.3 Codes

A *code* of *length* n on a finite alphabet A with q elements is a subset $\mathcal{C}$ of A^n. A *word* is an element of A^n, a *codeword* is an element of $\mathcal{C}$.

A *linear code* over a finite field $\mathbf{F}_q$ of length n and *dimension* r is a $\mathbf{F}_q$–vector subspace of $\mathbf{F}_q^n$ of dimension r (such a code is also called a (n,r)–code).

A subspace $\mathcal{C}$ of $\mathbf{F}_q^n$ of dimension r can be described by giving a basis $e_1, \ldots, e_r$ of $\mathcal{C}$ over $\mathbf{F}_q$, so that

$$\mathcal{C} = \{m_1 e_1 + \cdots + m_r e_r \ ; \ (m_1, \ldots, m_r) \in \mathbf{F}_q^r\}.$$

An alternative description of a subspace $\mathcal{C}$ of $\mathbf{F}_q^n$ of codimension $n - r$ is by giving $n - r$ linearly independent linear forms $L_1, \ldots, L_{n-r}$ in n variables $\underline{x} = (x_1, \ldots, x_n)$ with coefficients in $\mathbf{F}_q$, such that

$$\mathcal{C} = \ker L_1 \cap \cdots \cap \ker L_{n-r}.$$

The sender replaces his message $(m_1, \ldots, m_r) \in \mathbf{F}_q^r$ of length r by the longer message $m_1 e_1 + \cdots + m_r e_r \in \mathcal{C} \subset \mathbf{F}_q^n$ of length n. The receiver checks whether the message $\underline{x} = (x_1, \ldots, x_n) \in \mathbf{F}_q^n$ belongs to $\mathcal{C}$ by computing the $n - r$–tuple $\underline{L}(\underline{x}) = (L_1(\underline{x}), \ldots, L_{n-r}(\underline{x})) \in \mathbf{F}_q^{n-r}$. If there is no error during the transmission, then $\underline{x} \in \mathcal{C}$ and $L_1(\underline{x}) = \cdots = L_{n-r}(\underline{x}) = 0$. On the opposite, if the receiver observes that some $L_i(\underline{x})$ is non–zero, he knows that the received message has at least one error. The message with was sent was an element $\underline{c}$ of the code $\mathcal{C}$, the message received $\underline{x}$ is not in $\mathcal{C}$, the error is $\underline{\epsilon} = \underline{x} - \underline{c}$. The values of $\underline{L}(\underline{x})$ may enable him to correct the errors in case there are not too many of them. We only give examples. For simplicity we take $q = 2$: we consider *binary codes*.

The minimum distance $d(\mathcal{C})$ of a linear code $\mathcal{C}$ is the minimal weight of a non–zero element in $\mathcal{C}$.

3.4 First examples

Trivial codes of length n are $\mathcal{C} = \{0\}$ of dimension 0 and $\mathcal{C} = \mathbf{F}_q^n$ of dimension n.

Example 70. Repetition code of length 2 detecting one error.
$n = 2$, $r = 1$, rate $= 1/2$.

$$\mathcal{C} = \big\{(0,0),\ (1,1)\big\}, \qquad e_1 = (1,1), \qquad L_1(x_1, x_2) = x_1 + x_2.$$

Example 71. Repetition code of length 3 correcting one error.
$n = 3$, $r = 1$, rate $= 1/3$.

$$\mathcal{C} = \big\{(0,0,0),\ (1,1,1)\big\}, \qquad e_1 = (1,1,1),$$

$$L_1(\underline{x}) = x_1 + x_3,\ L_2(\underline{x}) = x_2 + x_3.$$

If the message which is received is correct, it is either $(0,0,0)$ or $(1,1,1)$, and the two numbers $L_1(\underline{x})$ and $L_2(\underline{x})$ are 0 (in $\mathbf{F}_2$). If there is exactly one mistake, then the message which is received is either one of

$$(0,0,1),\ (0,1,0),\ (1,0,0),$$

or else one of

$$(1,1,0),\ (1,0,1),\ (0,1,1).$$

In the first case the message which was sent was $(0,0,0)$, in the second case it was $(1,1,1)$.

A message with a single error is obtained by adding to a codeword one of the three possible errors

$$(1,0,0),\ (0,1,0),\ (0,0,1).$$

If the mistake was on x_1, which means that $\underline{x} = \underline{c} + \underline{\epsilon}$ with $\underline{\epsilon} = (1,0,0)$ and $\underline{c} \in \mathcal{C}$ a codeword, then $L_1(\underline{x}) = 1$ and $L_2(\underline{x}) = 0$. If the mistake was on x_2, then $\underline{\epsilon} = (0,1,0)$ and $L_1(\underline{x}) = 0$ and $L_2(\underline{x}) = 1$. Finally if the mistake was on x_3, then $\underline{\epsilon} = (0,0,1)$ and $L_1(\underline{x}) = L_2(\underline{x}) = 1$. Therefore, the three possible values for the pair $\underline{L}(\underline{x}) = (L_1(\underline{x}), L_2(\underline{x}))$ other than $(0,0)$ correspond to the three possible positions for a mistake. We will see that this is a perfect one error correcting code.

Example 72. Parity bit code detecting one error.

$n = 3$, $r = 2$, rate $= 2/3$.

$$\mathcal{C} = \left\{(m_1, m_2, m_1 + m_2)\ ;\ (m_1, m_2) \in \mathbf{F}_2^2\right\}$$

$$e_1 = (1,0,1),\ e_2 = (0,1,1), \qquad L_1(x_1,x_2,x_3) = x_1 + x_2 + x_3.$$

This is the easiest example of the *bit parity check.*

Example 73. A one error correcting code of dimension 5 using the parity bit idea.

$n = 5$, $r = 2$, rate $= 2/5$.

$$\mathcal{C} = \left\{(m_1, m_2, m_1, m_2, m_1 + m_2)\ ;\ (m_1, m_2) \in \mathbf{F}_2^2\right\}$$

$$e_1 = (1,0,1,0,1),\ e_2 = (0,1,0,1,1),$$

$$L_1(\underline{x}) = x_1 + x_3,\ L_2(\underline{x}) = x_2 + x_4,\ L_3(\underline{x}) = x_1 + x_2 + x_5,$$

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_1	x_2	x_3	x_4	x_5
$\underline{L}(\underline{x})$	$(1,0,1)$	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

Therefore, when there is a single error, the value of $\underline{L}(\underline{x})$ enables one to correct the error.

One may observe that a single error will never produce the triple $(1,1,0)$ nor $(1,1,1)$ for $\underline{L}(\underline{x})$: there are 8 elements $\underline{x} \in \mathbf{F}_2^5$ which cannot be received starting from a codeword and adding at most one mistake, namely $(x_1, x_2, x_1 + 1, x_2 + 1, x_5)$, with $(x_1, x_2, x_5) \in \mathbf{F}_2^3$.

Example 74. A one error correcting code of dimension 6 using the parity bit idea.

$n = 6$, $r = 3$, rate $= 1/2$.

$$\mathcal{C} = \left\{(m_1, m_2, m_3, m_2 + m_3, m_1 + m_3, m_1 + m_2)\ ;\ (m_1, m_2, m_3) \in \mathbf{F}_2^3\right\}$$

$$e_1 = (1,0,0,0,1,1),\ e_2 = (0,1,0,1,0,1),\ e_3 = (0,0,1,1,1,0),$$

$$L_1(\underline{x}) = x_2 + x_3 + x_4,\ L_2(\underline{x}) = x_1 + x_3 + x_5,\ L_3(\underline{x}) = x_1 + x_2 + x_6.$$

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_1	x_2	x_3	x_4	x_5	x_6
$\underline{L}(\underline{x})$	$(0,1,1)$	$(1,0,1)$	$(1,1,0)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

Therefore, when there is a single error, the value of $\underline{L}(\underline{x})$ enables one to correct the error.

One may observe that a single error will never produce the triple $(1,1,1)$ for $\underline{L}(\underline{x})$: there are 8 elements $\underline{x} \in \mathbf{F}_2^5$ which cannot be received starting from a codeword and adding at most one mistake, namely:

$$(x_1, x_2, x_3, x_2 + x_3 + 1, x_1 + x_3 + 1, x_1 + x_2 + 1) \quad \text{with} \quad (x_1, x_2, x_3) \in \mathbf{F}_2^3.$$

Example 75. Hamming Code of dimension 4 and length 7 over $\mathbf{F}_2$ correcting one error.

$n = 7$, $r = 4$, rate $= 7/4$, *corrects one error.*
$\mathcal{C}$ is the set of

$$(m_1, m_2, m_3, m_4, m_1 + m_2 + m_4, m_1 + m_3 + m_4, m_2 + m_3 + m_4) \in \mathbf{F}_2^7$$

where (m_1, m_2, m_3, m_4) ranges over $\mathbf{F}_2^4$. A basis of $\mathcal{C}$ is

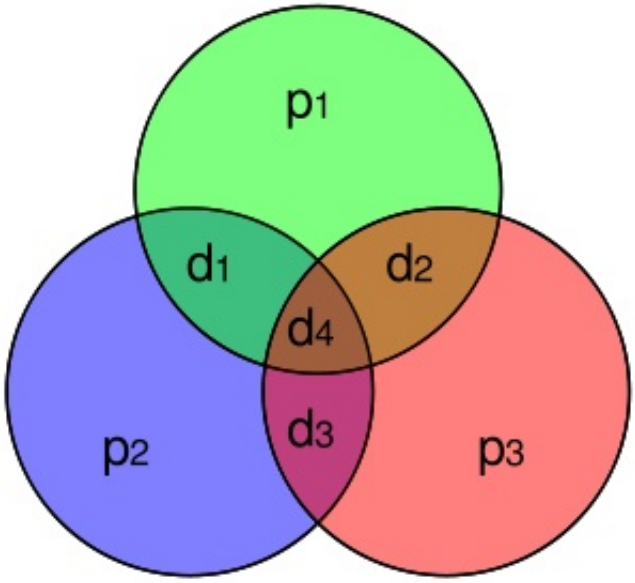
$$\begin{array}{ll} e_1 = (1,0,0,0,1,1,0), & e_2 = (0,1,0,0,1,0,1), \\ e_3 = (0,0,1,0,0,1,1), & e_4 = (0,0,0,1,1,1,1) \end{array}$$

and $\mathcal{C}$ is also the intersection of the hyperplanes defined as the kernels of the linear forms

$$L_1(\underline{x}) = x_1 + x_2 + x_4 + x_5,\ L_2(\underline{x}) = x_1 + x_3 + x_4 + x_6,\ L_3(\underline{x}) = x_2 + x_3 + x_4 + x_7.$$

This corresponds to the next picture from

`http://en.wikipedia.org/wiki/Hamming_code`



Hamming (7,4) code

The possible values for the triple $\underline{L}(\underline{x})$ corresponding to a single error are displayed in the following table.

$\underline{x}$	x_1	x_2	x_3	x_4	x_5	x_6	x_7
$\underline{L}(\underline{x})$	$(1,1,0)$	$(1,0,1)$	$(0,1,1)$	$(1,1,1)$	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$

This table gives a bijective map between the set $\{1,2,3,4,5,6,7\}$ of indices of the unique wrong letter in the word $\underline{x}$ which is received with a single mistake on the one hand, the set of values of the triple

$$\underline{L}(\underline{x}) = \big(L_1(\underline{x}), L_2(\underline{x}), L_3(\underline{x})\big) \in \mathbf{F}_2^3 \setminus \{0\}$$

on the second hand.

This is a *perfect* 1*–error correcting code.*

3.5 Cyclic codes

A *cyclic code* $\mathcal{C}$ of length n over an alphabet with q elements is a $\mathbf{F}_q$–vector subspace of $\mathbf{F}_q^n$ such that, for any $(a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathcal{C}$, the element $(a_n, a_1, a_2, \ldots, a_{n-1})$ also belongs to $\mathcal{C}$. We speak of a q-ary code as a reference to the number of elements of the alphabet; it is a binary code for $q = 2$, a ternary code for $q = 3$.

We denote by $T : \mathbf{F}_q^n \longrightarrow \mathbf{F}_q^n$ the linear map (*right shift*)

$$(a_1, a_2, \ldots, a_{n-1}, a_n) \longmapsto (a_n, a_1, a_2, \ldots, a_{n-1}).$$

In the group of automorphism of the $\mathbf{F}_q$–vector space $\mathbf{F}_q^n$, this element T satisfies $T^n = I$ (the unit of $\mathrm{Aut}(\mathbf{F}_q^n/\mathbf{F}_q)$, namely the identity map). This is how the polynomial $X^n - 1$ comes into the picture.

Assume $\gcd(n, q) = 1$. A natural basis of the $\mathbf{F}_q$–space $\mathbf{F}_q[X]/(X^n - 1)$ is given by the classes modulo $X^n - 1$ of $1, X, \ldots, X^{n-1}$. This gives a $\mathbf{F}_q$–isomorphism

$$\begin{array}{rccc} \Psi : & \mathbf{F}_q^n & \longrightarrow & \mathbf{F}_q[X]/(X^n-1) \\ & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}. \end{array}$$

Rewrite the definition of T with the indices $\{0, \ldots, n-1\}$ in place of $\{1, \ldots, n\}$:

$$T(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2});$$

hence,

$$\Psi \circ T(a_0, a_1, \ldots, a_{n-1}) = X(a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}) \mod X^n - 1.$$

As a consequence, a subset $\mathcal{C}$ of $\mathbf{F}_q^n$ is stable under the shift T if and only if $\Psi(\mathcal{C})$ is stable under multiplication by X in $\mathbf{F}_q[X]/(X^n - 1)$.

A vector subspace $\mathcal{I}$ of $\mathbf{F}_q[X]/(X^n - 1)$ is stable under multiplication by X if and only if $\mathcal{I}$ is an ideal of the quotient ring $\mathbf{F}_q[X]/(X^n - 1)$. Furthermore, there is a bijective map between the ideals of $\mathbf{F}_q[X]/(X^n - 1)$ and the ideals of $\mathbf{F}_q[X]$ which contain $X^n - 1$. Since the ring $\mathbf{F}_q[X]$ is principal, the ideals containing $X^n - 1$ are the ideals (Q) generated by a divisor Q of $X^n - 1$. Given such an ideal, there is a single generator Q which is monic. If d is the degree of Q, then the ideal of $\mathbf{F}_q[X]/(X^n - 1)$ generated by the class of Q modulo $X^n - 1$ is a $\mathbf{F}_q$–vector space of dimension $r = n - d$: a basis is $Q, XQ, \ldots, X^{r-1}Q$. Also, the following sequence of $\mathbf{F}_q$–linear maps is exact:

$$0 \longrightarrow \frac{(Q)}{(X^n-1)} \longrightarrow \frac{\mathbf{F}_q[X]}{(X^n-1)} \longrightarrow \frac{\mathbf{F}_q[X]}{(Q)} \longrightarrow 0.$$

The dimensions of these three vector spaces are r, n and d with $n = r + d$, as it should. Combining these results with Proposition 61, we deduce

Proposition 76. *Given a finite field $\mathbf{F}_q$ and an integer n with $\gcd(n, q) = 1$, there are bijective maps between the following subsets.*
(i) The cyclic codes $\mathcal{C}$ of length n over $\mathbf{F}_q$.
(ii) The ideals $\mathcal{I}$ of $\mathbf{F}_q[X]/(X^n - 1)$.
(iii) The monic divisors Q of $X^n - 1$ in $\mathbf{F}_q[X]$.
(iv) The subsets I of $\mathbf{Z}/n\mathbf{Z}$ which are stable under multiplication by q.
Under this correspondence, the dimension d of the code is the dimension of the $\mathbf{F}_q$–vector space $\mathcal{I}$, the degree of Q is $r = n - d$, and the number of elements in I is also r.

The trivial code $\{0\}$ of length n and dimension 0 corresponds to the ideal (0) of $\mathbf{F}_q[X]/(X^n - 1)$, to the divisor $X^n - 1$ of $X^n - 1$ and to the empty subset of $\mathbf{Z}/n\mathbf{Z}$.

The full code $\mathbf{F}_q^n$ of length n and dimension n corresponds to the ideal (1) of $\mathbf{F}_q[X]/(X^n-1)$, to the divisor 1 of X^n-1 and to the set $I=\mathbf{Z}/n\mathbf{Z}$ itself.

The repetition code $\{(a,a,\ldots,a)\ ;\ a\in\mathbf{F}_q\}\subset\mathbf{F}_q^n$ of length n and dimension 1, generalising examples (70) and (71) corresponds to the ideal $(1+X+\cdots+X^{n-1})$ of $\mathbf{F}_q[X]/(X^n-1)$, to the divisor $(X^n-1)/(X-1)$ of X^n-1 and to the set $I=(\mathbf{Z}/n\mathbf{Z})\setminus\{0\}$.

The hyperplane of equation $x_1+\cdots+x_n=0$ in $\mathbf{F}_q^n$ is a parity bit check code of length n and dimension $n-1$. It corresponds to the ideal $(X-1)$ of $\mathbf{F}_q[X]/(X^n-1)$, to the divisor $X-1$ of X^n-1 and to the subset $I=\{0\}$ of $\mathbf{Z}/n\mathbf{Z}$.

3.6 Detection, correction and minimal distance

A *transmission with at most t errors* is a mapping $f:\mathcal{C}\longrightarrow\mathbf{F}_q^n$ such that for all $\underline{c}\in\mathcal{C}$,

$$d\big(f(\underline{c}),\underline{c}\big)\leq t.$$

The *error* is $\epsilon(\underline{c})=f(\underline{c})-\underline{c}$. The message which is sent is $\underline{c}$, a codeword, the message which is received is $f(\underline{c})$.

The first question is to detect if an error occurred, that means to detect whether $\epsilon(\underline{c})$ is zero or not. A code $\mathcal{C}$ *can detect t errors* if for all $\underline{c}\in\mathcal{C}$,

$$B(\underline{c},t)\cap\mathcal{C}=\{\underline{c}\}.$$

This means that for a transmission $f:\mathcal{C}\longrightarrow\mathbf{F}_q^n$ with at most t errors, $f(\underline{c})\in\mathcal{C}$ if and only if $\epsilon(\underline{c})=0$. The receiver checks whether $f(\underline{c})$ is in $\mathcal{C}$ or not (for instance, by using a check matrix H). If $f(\underline{c})\in\mathcal{C}$, if the code is t–error detecting and if the transmission had at most t errors, then $\epsilon(\underline{c})=0$: there was no error.

A code $\mathcal{C}$ of length n over $\mathbf{F}_q$ *can correct t errors* (one also says that it is *t–error correcting*) if for all $\underline{x}\in\mathbf{F}_q^n$,

$$\#B(\underline{x},t)\cap\mathcal{C}\leq 1.$$

This means that any transmission $f:\mathcal{C}\longrightarrow\mathbf{F}_q^n$ with at most t errors is injective: for all $\underline{y}\in f(\mathcal{C})$ there is a single $\underline{c}$ such that $\underline{y}=f(\underline{c})$. After receiving $\underline{y}=f(\underline{c})$, knowing that the transmission had at most t errors, the receiver computes the unique $\underline{c}$ for which $d(y;\underline{c})\leq t$. Then he knows that $f(\underline{c})=\underline{y}$ and he also knows the error $\epsilon(\underline{c})=f(\underline{c})-\underline{y}$.

Lemma 77. *A code $\mathcal{C}$ of length n over $\mathbf{F}_q$ can detect t errors if and only if $d(\mathcal{C})\geq t+1$. The code $\mathcal{C}$ can correct t errors if and only if $d(\mathcal{C})\geq 2t+1$.*

Proof. The condition $d(\mathcal{C})\geq t+1$ means that a word at Hamming distance at most t from an element $\underline{c}$ of $\mathcal{C}$ and distinct from $\underline{c}$ does not belong to $\mathcal{C}$. This is equivalent to saying that $\mathcal{C}$ can detect t errors.

For the second part of Lemma 77, assume first that $d(\mathcal{C})\geq 2t+1$. Let $\underline{x}\in\mathbf{F}_q^n$ and let $\underline{c}_1$ and $\underline{c}_2$ in $\mathcal{C}$ satisfy $d(\underline{x},\underline{c}_1)\leq t$ and $d(\underline{x},\underline{c}_2)\leq t$. Then by the triangle inequality

$$d(\underline{c}_1,\underline{c}_2)\leq 2t<d(\mathcal{C}).$$

Therefore, $\underline{c}_1 = \underline{c}_2$.
Conversely, assume $d(\mathcal{C}) \leq 2t$: there is a non–zero element $\underline{c}$ in $\mathcal{C}$ with $w(\underline{c}) \leq 2t$, hence, $\underline{c}$ has at most $2t$ non–zero components. Split the set of indices of the non–zero components of $\underline{c}$ into two disjoint subsets I_1 and I_2 having each at most t elements. Next define $\underline{x} \in \mathbf{F}_q^n$ as the point having the same components x_i as $\underline{c}$ for $i \in I_1$ and 0 for i not in I_1. Then in the Hamming ball of center $\underline{x}$ and radius t there are at least two points of $\mathcal{C}$, namely 0 and $\underline{c}$. Hence, $\mathcal{C}$ is not t–error correcting. □

Proposition 78. *For a code $\mathcal{C}$ of length n and dimension d, the minimum distance is bounded by*

$$d(\mathcal{C}) \leq n + 1 - d.$$

Proof. The subspace

$$V = \{(x_1, \ldots, x_{n+1-d}, 0, \ldots, 0)\ ;\ (x_1, \ldots, x_{n+1-d}) \in \mathbf{F}_q^{n+1-d}\}$$

of $\mathbf{F}_q^n$ has dimension $n + 1 - d$, the sum of this dimension with the dimension d of $\mathcal{C}$ exceeds the dimension n of the ambient space $\mathbf{F}_q^n$, hence, there is a non–zero element in the intersection. This is a non–zero element of $\mathcal{C}$ with weight $\leq n + 1 - d$. □

A code $\mathcal{C}$ of length n and dimension d for which $d(\mathcal{C}) = n + 1 - d$ is called MDS (*Maximal Distance Separable*). Examples (70), (71) and (72) are MDS codes.

Hamming code of length 7 and dimension 4 (Example 75 and § 3.7) has minimum distance 3, hence, is not MDS.

From (69), we deduce Hamming's bound on the error correcting capacity of a code of length n and dimension r over $\mathbf{F}_q$ (see [7] Theorem 3.3.1).

Theorem 79. *For a linear code $\mathcal{C}$ in $\mathbf{F}_q^n$ of dimension r which is t–error correcting,*

$$1 + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \leq q^{n-r}.$$

A t–error correcting code over $\mathbf{F}_q$ of length n is *perfect* if this upper bound is an equality, meaning that $\mathbf{F}_q^n$ is the disjoint union of the balls of radius t around the codewords in $\mathcal{C}$.

For a perfect 1–error correcting code over $\mathbf{F}_q$ of length n and dimension d, the union of the q^d Hamming balls of radius 1 gives a packing of the set $\mathbf{F}_q^n$ with q^n elements, hence,

$$q^d\big(1 + n(q-1)\big) = q^n.$$

We set $d = n - r$, so that $n = (q^r - 1)/(q - 1)$. One easily checks that the order of q modulo n is r. According to Theorem 45, the polynomial $\Phi_n(X)$, splits into irreducible factors of degree r. Each of these factors gives a cyclic code which is Hamming q-ary code of length n and dimension d.

For instance, take $q = 2$. For $r = 2$ we have $n = 3$, $d = 1$ and this is the repetition code $\{(0,0,0)\ ,\ (1,1,1)\}$ of example (71). For $r = 3$ we have $n = 7$, $d = 4$ which are the parameters of Hamming code considered in example 75 and § 3.7.

3.7 Hamming codes

From `http://en.wikipedia.org/wiki/Hamming_code`

> *In telecommunication, a Hamming code is a linear error-correcting code named after its inventor, Richard Hamming. Hamming codes can detect up to two simultaneous bit errors, and correct single-bit errors; thus, reliable communication is possible when the Hamming distance between the transmitted and received bit patterns is less than or equal to one. By contrast, the simple parity code cannot correct errors, and can only detect an odd number of errors.*
>
> *Hamming worked at Bell Labs in the 1940s on the Bell Model V computer, an electromechanical relay-based machine with cycle times in seconds. Input was fed in on punch cards, which would invariably have read errors. During weekdays, special code would find errors and flash lights so the operators could correct the problem. During after-hours periods and on weekends, when there were no operators, the machine simply moved on to the next job.*
>
> *Hamming worked on weekends, and grew increasingly frustrated with having to restart his programs from scratch due to the unreliability of the card reader. Over the next few years he worked on the problem of error-correction, developing an increasingly powerful array of algorithms. In 1950 he published what is now known as Hamming Code, which remains in use in some applications today.*

Let $\mathbf{F}_q$ be a finite field with q elements and let r be a positive integer. Define

$$n = \frac{q^r - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{r-1}.$$

Therefore, q is prime to n and the class of q in $(\mathbf{Z}/n\mathbf{Z})^\times$ has order r. The subset $I = \{1, q, q^2, \ldots, q^{r-1}\}$ of $\mathbf{Z}/n\mathbf{Z}$ is stable under multiplication by q. This defines a code of length n and dimension $d = n - r$ over $\mathbf{F}_q$.

We first develop the special case already considered in example 75, where $r = 3$, $q = 2$, hence, $n = 7$ and $d = 4$. We have seen in example 51 that the decomposition of Φ_7 over $\mathbf{F}_2$ is

$$\Phi_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1).$$

We choose $Q(X) = 1 + X + X^3$. The vector of its coordinates in the basis $1, X, X^2, X^3, X^4, X^5, X^6$ is $e_0 = (1,1,0,1,0,0,0) \in \mathbf{F}_2^7$. Next define e_1, e_2 and

e_3 by taking the coordinates in the same basis of XQ, X^2Q, X^3Q:

$$\begin{array}{rl} Q(X) = 1 + X + X^3 & e_0 = (1,1,0,1,0,0,0), \\ XQ(X) = X + X^2 + X^4, & e_1 = (0,1,1,0,1,0,0) = Te_0, \\ X^2Q(X) = X^2 + X^3 + X^5, & e_2 = (0,0,1,1,0,1,0) = Te_1, \\ X^3Q(X) = X^3 + X^4 + X^6, & e_3 = (0,0,0,1,1,0,1) = Te_2. \end{array}$$

The components of e_0, e_1, e_2, e_3 in $\mathbf{F}_2^7$ are the rows of the following matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The elements in the code $\mathcal{C}$ are the 16 elements

$$m_0e_0 + m_1e_1 + m_2e_2 + m_3e_3$$

with $(m_0, m_1, m_2, m_3) \in \mathbf{F}_2^4$. This subspace $\mathcal{C}$ of $\mathbf{F}_2^7$ has dimension 4, hence, it is an intersection of 3 hyperplanes. Let us recall how to find a basis of the $\mathbf{F}_q$–vector space of linear forms vanishing on a subspace V of F^n given by a basis with d elements. We write the $d \times n$ matrix whose rows are the coordinates of the given basis. We add one further row with the variables $x_1, \ldots, x_n$. By elementary columns operations (replacing a column by its sum with a linear combination of the other columns, which corresponds to the multiplication on the right by a regular $n \times n$ matrix), we get a matrix of the form

$$\begin{pmatrix} & I_d & & 0 & \ldots & 0 \\ y_1 & y_2 & \ldots & y_d & y_{d+1} & \ldots & y_n \end{pmatrix}$$

where I_d is the identity $d \times d$ matrix and $y_1, \ldots, y_n$ are linearly independent linear forms in $x_1, \ldots, x_n$. Then the $(n-d)$–tuple $y_{d+1}, \ldots, y_n$ is a basis of the space of linear forms vanishing on V. This can be checked by reducing to the simple case of a hyperplane $x_n = t_1x_1 + \cdots + t_{n-1}x_{n-1}$ with $d = n-1$ and the matrix

$$\begin{pmatrix} & & & t_1 \\ & I_{n-1} & & \vdots \\ & & & t_{n-1} \\ x_1 & x_2 & \ldots & x_{n-1} & x_n \end{pmatrix}$$

We perform this process with the matrix G: therefore, we introduce

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix}.$$

Here is the last row of the successive matrices obtained by the triangulation process (we work over $\mathbf{F}_2$)

$$\begin{array}{ccccccc}
x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\
x_0 & x_1+x_0 & x_2 & x_3+x_0 & x_4+x_0+x_1 & x_5 & x_6 \\
x_0 & x_1+x_0 & x_2+x_0+x_1 & x_3+x_0 & x_4+x_0+x_1 & x_5 & x_6 \\
x_0 & x_1+x_0 & x_2+x_0+x_1 & x_3+x_1+x_2 & x_4+x_0+x_1 & x_5+x_0+x_1+x_2 & x_6 \\
x_0 & x_1+x_0 & x_2+x_0+x_1 & x_3+x_1+x_2 & x_4+x_0+x_2+x_3 & x_5+x_0+x_1+x_2 & x_6 \\
x_0 & x_1+x_0 & x_2+x_0+x_1 & x_3+x_1+x_2 & x_4+x_0+x_2+x_3 & x_5+x_0+x_1+x_2 & x_6+x_1+x_2+x_3
\end{array}$$

Hence, we introduce the three linear forms

$$\begin{aligned}
L_0(\underline{x}) &= x_0+x_2+x_3+x_4 \\
L_1(\underline{x}) &= x_0+x_1+x_2+x_5 \\
L_2(\underline{x}) &= x_1+x_2+x_3+x_6.
\end{aligned}$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{80}$$

The 7 column vectors are all the non–zero elements in $\mathbf{F}_2^3$. The product $G \cdot {}^tH$ of G with the transpose of H is the zero 4×3 matrix.

The same construction can be performed in the general case of $\mathbf{F}_q^n$ with $n = (q^r-1)/(q-1)$. In $\mathbf{F}_q^r$, there are q^r-1 non–zero elements, each of them defines a line ($\mathbf{F}_q$–subspace of dimension 1) having $q-1$ non–zero elements, and, therefore, there are n lines: on each of them we select one element. We take for H the $r \times n$ matrix whose columns are the coordinates of these elements. Any two rows of H are linearly independent over $\mathbf{F}_q$. The intersection of the r hyperplanes $\mathbf{F}_q^n$ defined by the rows of H is a code which is *Hamming code of length n and dimension $d = n-r$ over $\mathbf{F}_q$*. The corresponding subset I of $\mathbf{Z}/n\mathbf{Z}$ is $\{1, q, q^2, \ldots, q^{r-1}\}$. Let ζ be a primitive n–th root of unity. Given a message $(m_r, \ldots, m_{n-1}) \in \mathbf{F}_q^d$, one computes $(m_0, \ldots, m_{r-1}) \in \mathbf{F}_q^r$, so that

$$m_0 + m_1\zeta + \cdots + m_{r-1}\zeta^{r-1} = -m_r\zeta^r - \cdots - m_{n-1}\zeta^{n-1}$$

and the associated codeword is $\underline{c} = (m_0, \ldots, m_{n-1}) \in \mathbf{F}_q^n$. For $\underline{x} \in \mathbf{F}_q^n$, we have

$$\underline{x} = (x_0, \ldots, x_n) \in \mathcal{C} \quad \text{ if and only if } \quad \sum_{i=0}^{n-1} x_i\zeta^i = 0.$$

If this sum is nonzero and if there exists $\underline{c} \in \mathcal{C}$ with $d(\underline{x}, \underline{c}) \leq 1$, then the error $\epsilon = \underline{x} - \underline{c} = (0, \ldots, 0, \epsilon_k, 0, \ldots, 0) \in \mathbf{F}_q^n$ has its nonzero component in position k with

$$\epsilon_k\zeta^k = -\sum_{i=0}^{n-1} x_i\zeta^i.$$

3.8 Generator matrix and check matrix

Among many others, a reference for this section is [7], Chapter 3.

Given a linear code $\mathcal{C}$ of dimension d and length n over $\mathbf{F}_q$, a *generator matrix* is a $d \times n$ matrix G with coefficients in $\mathbf{F}_q$, the rows of which are the components of a basis of $\mathcal{C}$. The code is the set of elements $\underline{m}G$ where $\underline{m}$ ranges over $\mathbf{F}_q^d$ (viewed as a $1 \times d$ row vector). From the definition, it follows that G has rank d.

A *check matrix* is a $(n-d) \times n$ matrix H with coefficients in $\mathbf{F}_q$, the rows of which are the components of a basis of the space of linear forms vanishing on $\mathcal{C}$. The code $\mathcal{C}$ is the set of elements $\underline{c}$ in $\mathbf{F}_q^n$ such that $H \cdot {}^t\underline{c} = 0$, where ^{t} denotes the transposition, so that ${}^t\underline{c}$ is a $n \times 1$ column vector in $\mathbf{F}_q^n$. Therefore,

$$G \cdot {}^tH = 0$$

where G is a $d \times n$ matrix of rank d and H a $r \times n$ matrix of rank $r = n - d$.

The code is said to be *in systematic form* if $H = \begin{pmatrix} A & I_r \end{pmatrix}$, where I_r is the identity $r \times r$ matrix and A is a $r \times d$ matrix.

Two codes are *isomorphic* if they have the same check matrix in suitable bases - for instance, the two descriptions that we gave of the Hamming code of length 7 and dimension 4 in example 75 and § 3.7 are isomorphic.

3.9 Further examples

3.9.1 The binary Golay code of length 23, dimension 12

A perfect code with $q = 2$, $n = 23$, $d = 12$ and minimal distance 7 (hence, it is 3–error correcting but not MDS) has been constructed by Golay as follows.

We have $2^{11} - 1 = 23 \times 89 = 2047$, which is the smallest integer of the form $M_p = 2^p - 1$ with p prime but which is not itself a prime (primes of the form $M_p = 2^p - 1$ are called *Mersenne primes*). We take the subset I of $(\mathbf{Z}/23\mathbf{Z})^\times$ generated by 2, which is

$$I = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

The decomposition of Φ_{23} over $\mathbf{F}_2$ has been given in exercise 54.

There are 2^{12} codewords, for each of them the Hamming ball of radius 3 has

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 1 + 23 + 253 + 1771 = 2048 = 2^{11}$$

elements, these balls are disjoint and the total number of elements in their union is $2^{11}2^{12} = 2^{23}$.

3.9.2 The ternary Golay code of length 11, dimension 6

An other perfect code constructed by Golay has the parameters $q = 3$, $n = 11$, $d = 6$ and minimal distance 5 (it is 2–error correcting not MDS). We have $3^5 - 1 = 11 \times 23$. We take the subset I of $(\mathbf{Z}/11\mathbf{Z})^\times$ generated by 3, which is $I = \{1, 3, 4, 5, 9\}$. The decomposition of Φ_{11} over $\mathbf{F}_3$ has been given in exercise 53.

There are 3^6 codewords, for each of them the Hamming ball of radius 2 has

$$\binom{11}{0} + 2\binom{11}{1} + 2^2\binom{11}{2} = 1 + 22 + 220 = 243 = 3^5$$

elements, they are disjoint the total number of elements in $\mathbf{F}_3^{11}$ is $3^6 3^5 = 3^{11}$.

3.9.3 BCH (Bose–Chaudhuri–Hocquenghem) codes

Given a finite field $\mathbf{F}_q$ and an integer r, let n be a divisor of $q^r - 1$. Hence, the order of q modulo n divides r. Let $\zeta \in \mathbf{F}_q^r$ be a primitive n-th root of unity and let $\delta \geq 2$ be an integer. Consider the morphism of rings

$$\begin{array}{ccc} \mathbf{F}_q[X]/(X^n - 1) & \longrightarrow & \mathbf{F}_q^{\delta-1} \\ P & \longmapsto & \big(P(\zeta^j)\big)_{1 \leq j \leq \delta - 1} \end{array}$$

The kernel is a cyclic q–ary code of length n and minimal distance δ, the generating polynomial is the lcm of the minimal polynomials over $\mathbf{F}_q$ of the elements ζ^j, $1 \leq j \leq \delta - 1$: the subset I of $\mathbf{Z}/n\mathbf{Z}$ is the smallest subset containing $\{1, \ldots, q\}$ and stable under multiplication by q.

3.9.4 Reed–Solomon code

The Reed–Solomon codes are special cases of BCH codes. Let $q = 2^m$, $n = q - 1$ and let ζ be a primitive n–th–th root of unity, that means a generator of $\mathbf{F}_q^\times$. For $1 \leq d \leq n$ the code associated with the subset $I = \{1, 2, 3, \ldots, n - d\}$ of $\mathbf{Z}/n\mathbf{Z}$ and to the polynomial

$$\prod_{i=1}^{n-d} (X - \zeta^i)$$

has dimension d and minimal distance $q - d$. This code is MDS; it is used in CD's. This code is specially efficient when errors occur often consecutively, since the words here have length m.

It is known that the only perfect codes are

- *The trivial code with a single element* 0.
- *The full code* $\mathbf{F}_q^n$.
- *A binary repetition code with odd length (see [7] Exercise 3.12).*
- *For* $r \geq 2$*, the* q*-ary Hamming code of length* $n = (q^r - 1)/(q - 1)$*, dimension* $n - r$*, and minimal distance* 3.
- *The ternary Golay code over* $\mathbf{F}_3$ *of length* 11*, dimension* 6 *and minimal distance* 5.
- *The binary Golay code over* $\mathbf{F}_2$ *of length* 23*, dimension* 12 *and minimal distance* 7.

3.10 Minimum distance of a code

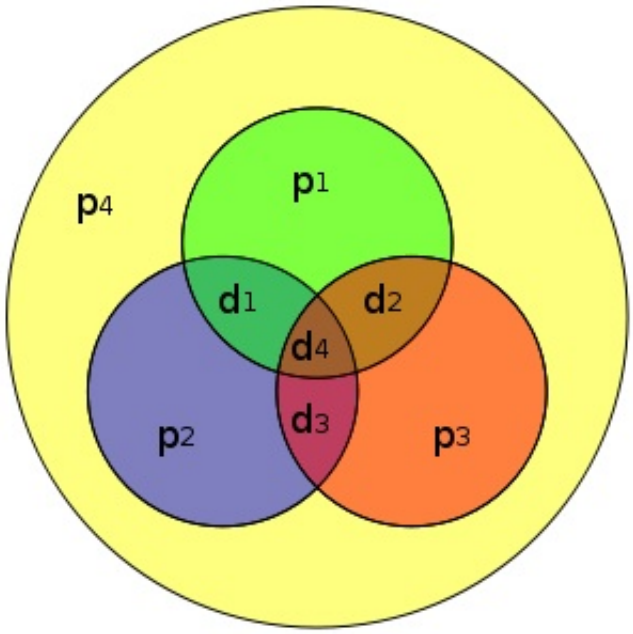
We state two results which are useful tools to compute the minimum distance of a code. For the first one, see [1], Prop. 11C.

Proposition 81. *Let $\mathcal{C}$ be a linear code over $\mathbf{F}_q$ of length n with check matrix H and let s be a positive integer. Then $\mathcal{C}$ has minimum distance $\geq s+1$ if and only if any s columns of H are linearly independent over $\mathbf{F}_q$.*

As a consequence, if any s columns of H are linearly independent over $\mathbf{F}_q$, and if further there exists $s+1$ columns of H which are linearly dependent over $\mathbf{F}_q$, then $d(\mathcal{C}) = s+1$. This enables one to check that Hamming code has minimum distance 3. Indeed in the matrix (80) all rows are non–zero and distinct (hence, any two rows are linearly independent over $\mathbf{F}_2$), but there are sets of three rows which are linearly dependent. If we add a row with 1's, then for the new matrix any sum of an odd number of rows is non–zero, hence, any three rows are linearly independent. This means that we extend the code of Hamming of lenth 7 to a code of length 8 by adding a parity check bit.

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}. \qquad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

This code has, therefore, minimum distance 4, it cannot correct more than one error, but it can detect up to 3 errors.



Hamming extended (8,4) code

To any code $\mathcal{C} \subset \mathbf{F}_q^n$ we can associate an *extended code* $\widetilde{\mathcal{C}} \subset \mathbf{F}_q^{n+1}$ by adding a parity bit:

$$\widetilde{\mathcal{C}} = \{(x_1, \ldots, x_{n+1}) \in \mathcal{C} \times \mathbf{F}_q \ ; \ (x_1, \ldots, x_n) \in \mathcal{C}, \ x_1 + \cdots + x_{n+1} = 0\} \subset \mathbf{F}_q^{n+1}.$$

One can check $d(\mathcal{C}) \leq d(\widetilde{\mathcal{C}}) \leq d(\mathcal{C})$.

A variant is to take the *even subcode*

$$\mathcal{C}' = \{(x_1, \ldots, x_n) \in \mathcal{C} \ ; \ x_1 + \cdots + x_n = 0\} \subset \mathbf{F}_q^n.$$

Then $d(\mathcal{C}) \leq d(\mathcal{C}')$.

Proposition 82. *Let $\mathcal{C}$ be a cyclic linear code of length n over $\mathbf{F}_q$ associated with a subset I of $\mathbf{Z}/n\mathbf{Z}$ stable under multiplication by q. Assume that there exist i and s such that $\{i+1, i+2, \ldots, i+s\} \subset I$. Then $d(\mathcal{C}) \geq s+1$.*

For instance, Hamming code is associated with the subset $I = \{1, 2, 4, \ldots, 2^{r-1}\}$ of $\mathbf{Z}/n\mathbf{Z}$, with two consecutive elements, hence, its distance is at least 3 (and here it is just 3).

4 Further exercises

Exercise 83. (a) Write the decomposition of the polynomial $X^{12} - 1$ into irreducible factors over $\mathbf{Z}$.
(b) Write the decomposition of the polynomial $X^{12} - 1$ into irreducible factors over the finite field $\mathbf{F}_5$ with 5 elements.
(c) How many elements are there in the splitting field over $\mathbf{F}_5$ of the polynomial $X^{12} - 1$?
(d) Let p be a prime number and $\mathbf{F}_p$ the finite field with p elements. What are the degrees of the irreducible factors of $X^{12} - 1$ over $\mathbf{F}_p$?

Exercise 84. (a) What are the degrees of the irreducible factors of the cyclotomic polynomials Φ_5, Φ_7 and Φ_{11} over $\mathbf{F}_2$? Over $\mathbf{F}_3$?
(b) Decompose the polynomial Φ_{15} into irreducible factors over $\mathbf{F}_2$.
(c) Is the polynomial $X^4 + X + 1$ irreducible over $\mathbf{F}_4$? over $\mathbf{F}_8$?
(d) For each of the fields $\mathbf{F}_2$, $\mathbf{F}_4$, $\mathbf{F}_8$ and $\mathbf{F}_{16}$, give the list of irreducible cyclotomic polynomials.

Exercise 85. Let $\mathbf{F}_q$ the finite field with q elements. Show that the number of squarefree monic polynomials in $\mathbf{F}_q[X]$ of degree n is

$$\begin{cases} 1 & \text{for } n = 0, \\ q & \text{for } n = 1, \\ q^n - q^{n-1} & \text{for } n \geq 2. \end{cases}$$

Exercise 86. Check that over the field $\mathbf{F}_3$ with 3 elements, the cyclotomic polynomial Φ_{728} splits into a product of 48 irreducible factors, each of which has degree 6.

Exercise 87. Check that if α is any root of the polynomial $X^3 + X + 1$ in characteristic 5, then 2α is a primitive root of the cubic extension $\mathbf{F}_{5^3}$ of $\mathbf{F}_5$.

Exercise 88. Let $\mathbf{F}_q$ be a finite field with q elements of characteristic p.
(a) Let K be a field containing $\mathbf{F}_q$ and let $\zeta \in K$ satisfy $\zeta^{q-1} = -1$. Check $\zeta^2 \in \mathbf{F}_q^\times$.
(b) How many irreducible factors are there in the decomposition of the polynomial $X^{2q-1} - X$ over $\mathbf{F}_q$?

Which are their degrees?

`Hint.` *Consider separately the case where $p = 2$ is even and the case where it is odd.*

Exercise 89. Given a finite field F with q elements, determine all integers n such that $x \mapsto x^n$ is an automorphism of F.

Exercise 90. (a) Let p and q be two prime numbers. Assume q divides $2^p - 1$. Check $q \equiv 1 \bmod p$.
(b) Let n be a positive integer and q a prime number. Assume that q divides $2^{2^n} + 1$. Check $q \equiv 1 \bmod 2^{n+1}$.

Exercise 91. Let p be a prime number and $f \in \mathbf{Z}[X]$ a polynomial. Check that the following conditions are equivalent.

(i) For all $a \in \mathbf{Z}$, $f(a) \equiv 0 \bmod p$.

(ii) There exist two polynomials g and h in $\mathbf{Z}[X]$ such that

$$f(X) = (X^p - X)g(X) + ph(X).$$

Exercise 92. Let p be a prime number Consider the endomorphism f of the multiplicative group $(\mathbf{Z}/p^2\mathbf{Z})^\times$ given by $x \to x^p$:

$$\begin{array}{rccc} f: & (\mathbf{Z}/p^2\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/p^2\mathbf{Z})^\times \\ & x & \longmapsto & x^p \end{array}$$

What are the image and kernel (and their number of elements)?

Exercise 93.
(a) Check that any element in $\mathrm{GL}_n(\mathbf{F}_q)$ has order $\leq q^n - 1$. Give an example where the order does not divide $q^n - 1$.
(b) Show that for $A \in \mathrm{GL}_n(\mathbf{F}_q)$, the following conditions are equivalent:
(i) A has order $q^n - 1$
(ii) The subring $\mathbf{F}_q[A]$ of $\mathrm{Mat}_{n\times n}(\mathbf{F}_q)$ generated by A is a field and A is a primitive element in this field.
(iii) The characteristic polynomial $\det(XI_n - A) \in \mathbf{F}_q[X]$ of A is a primitive polynomial.

Exercise 94. Let $m \in \mathbf{Z}$, $1 \leq m \leq 12$. Does there exist a domain A (commutative ring without zero divisor) such that the group of units of A has m elements?

Exercise 95. Let $\mathbf{F}_q$ be a finite field and $f \in \mathbf{F}_q[X]$ be a monic irreducible polynomial with $f(X) \neq X$.
(a) Show that the roots α of f in $\overline{\mathbf{F}}_p$ all have the same order in the multiplicative group $\overline{\mathbf{F}}_p^\times$. We denote this order by $p(f)$ and call it the *period* of f.
(b) For ℓ a positive integer, check that $p(f)$ divides ℓ if and only if $f(X)$ divides $X^\ell - 1$.
(c) Check that if f has degree n, then $p(f)$ divides $q^n - 1$. Deduce that q and $p(f)$ are relatively prime.
(d) A monic irreducible polynomial f is *primitive* if its degree n and its period $p(f)$ are related by $p(f) = q^n - 1$. Explain the definition.
(e) Recall that $X^2 + X + 1$ is the unique irreducible polynomials of degree 2 over $\mathbf{F}_2$, that there are two irreducible polynomials of degree 3 over $\mathbf{F}_2$:

$$X^3 + X + 1, \quad X^3 + X^2 + 1,$$

three irreducible polynomials of degree 4 over $\mathbf{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad X^4 + X^3 + X^2 + X + 1$$

and three monic irreducible polynomials of degree 2 over $\mathbf{F}_3$:

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1.$$

For each of these 9 polynomials compute the period. Which ones are primitive?
(f) Which are the irreducible polynomials over $\mathbf{F}_2$ of period 15? Of period 5?

Exercise 96. Let $\mathbf{F}_p$ be the prime field with p elements and let ℓ be a prime number. Show that if $a \in \mathbf{F}_p$ is not an ℓ–th power in $\mathbf{F}_p$, then $x^\ell - a$ is irreducible over $\mathbf{F}_p$.

Exercise 97. Let $u \in \mathbf{F}_p^\times$. Check that the polynomial $X^p - X - u$ is irreducible over $\mathbf{F}_p$.

Exercise 98. *(Galois Theorem)* Let p be a prime number and P a polynomial of $\mathbf{F}_p[X]$ of degree $n \geq 1$ such that $P(0) \neq 0$. The goal is to prove that there exist $m < p^n$ such that P divides $X^m - 1$.
(a) Using Euclidean division, show that there exists k with $1 \leq k \leq p^n$ such that P divides $X^k - 1$.
(b) Show that one may select $k < p^n$.
(c) Find the integer $m < 8$ such that $X^3 + X + 1$ divides $X^m - 1$ in $\mathbf{F}_2[X]$.

Exercise 99. Let $u \in \mathbf{F}_p^\times$. Denote by m the order of u in $\mathbf{F}_p^\times$. Set $k = (p-1)/m$.
(a) Show that in the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbf{F}_p$, all factors have degree m
(b) Show that there are k elements $v_1, \ldots, v_k$ in $\mathbf{F}_p^\times$ such that $v_i^k = u$.
(c) Write the the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbf{F}_p$.

Exercise 100. Decompose the polynomial $X^{p+1} - 1$ into irreducible polynomials over $\mathbf{F}_p$.

Exercise 101. How many $(x, y) \in \mathbf{F}_8^2$ are there satisfying

$$x^3y + y^3 + x = 0?$$

Exercise 102. For each of the following values of p (a prime number), r (a positive integer, $q = p^r$) and n a positive integer,
(1) Give the list of monic irreducible polynomials of degree n over the field $\mathbf{F}_q$
(2) Select a primitive root of unity of order $q^n - 1$ in $\mathbf{F}_{q^n}$ and write the table of discrete logarithms of basis α
(3) For each of the polynomials listed in (1), give the list of its roots in $\mathbf{F}_{q^n}$
(4) If $r \neq 1$, decompose each polynomials of degree rn over $\mathbf{F}_p$ into irreducible factors over $\mathbf{F}_q$.

p	r	n
2	1	2
3	1	2
5	1	2
7	1	2
2	1	3
3	1	3
2	2	2
3	2	2
2	3	2

Exercise 103. Let $\mathbf{F}_q$ be a finite field with q elements of characteristic $\neq 5$. How many cyclic codes are there on $\mathbf{F}_q$ of dimension 5? What are their dimensions?

Exercise 104. Let r be a positive integer. Denote by n_r the least positive integer such that $2^{n-r} \geq 1 + n$.
(a) Show that for $n < n_r$ there is no 1–error correcting code on $\mathbf{F}_{2^n}$ of dimension r.
(b) For each of the values $r = 0, 1, 2, 3, 4$, give an example of a 1–error correcting code on $\mathbf{F}_{2^{n_r}}$ of dimension r.

Exercise 105. What is the least positive integer n such that there exists a 1–error correcting code of length n?

Exercise 106. Let $f : \mathbf{F}_3^2 \to \mathbf{F}_3^4$ be the linear map

$$F(a, b) = (a, b, a + b, a - b)$$

and $\mathcal{C}$ be the image of f.
(a) What are the length and the dimension of the code $\mathcal{C}$? How many elements are there in $\mathcal{C}$? List them.

(b) What is the minimum distance $d(\mathcal{C})$ of $\mathcal{C}$? How many errors can the code $\mathcal{C}$ detect? How many errors can the code $\mathcal{C}$ correct? Is it a MDS code?
(c) How many elements are there in a Hamming ball of $\mathbf{F}_3^4$ of radius 1? Write the list of elements in the Hamming ball of $\mathbf{F}_3^4$ of radius 1 centered at $(0,0,0,0)$.
(d) Check that for any element $\underline{x}$ in $\mathbf{F}_3^4$, there is a unique $\underline{c} \in \mathcal{C}$ such that $d(\underline{c}, \underline{x}) \leq 1$.
What is $\underline{c}$ when $\underline{x} = (1, 0, -1, 1)$?

Exercise 107. Let $\mathbf{F}_q$ be a finite field with q elements. Assume $q \equiv 3 \bmod 7$. How many cyclic codes of length 7 are there on $\mathbf{F}_q$? For each of them describe the code: give its dimension, the number of elements, a basis, a basis of the space of linear forms vanishing on it, its minimum distance, the number of errors it can detect or correct and whether it is MDS or not.

Exercise 108. Let $(P_i)_{i \in I}$ be a family of polynomials with coefficients in $\mathbf{Z}$. Show that the following properties are equivalent.
(a) The P_i 's have a common zero in $\mathbf{C}$.
(b) There exists an infinite set of primes p such that the P_i 's have a common zero in $\mathbf{F}_p$.
(c) For every prime p, except a finite number, there exists a field of characteristic p in which the P_i's have a common zero.
Example with a family having a single element P. Show that for the polynomial $P(X) = X^2 - 5$ there are infinitely many p for which the congruence $P(x) \equiv 0 \bmod p$ has a solution $x \in \mathbf{Z}$, and there are also infinitely many p for which the congruence $P(x) \equiv 0 \bmod p$ has no solution $x \in \mathbf{Z}$.
`Reference`: Jean-Pierre Serre, *How to use finite fields for problems concerning infinite fields*,
`http://arxiv.org/abs/0903.0517`
`Hint.`
Let n be the number of variables.
`(a) implies (b).` Assume (a). Show that there is a number field K in which the P_i's have a common zero $\underline{\alpha} \in K^n$. Using Chebotarev density Theorem, show that there exist infinitely many prime numbers p totally split in K such that the reduction of $\underline{\alpha}$ modulo a prime ideal above p in K is well defined and produces a common zero of the P_i's in $\mathbf{F}_p^n$. Deduce (b).
`(a) implies (c).` Use the same argument but without the condition that p splits completely in K.
`(b) or (c) implies (a).` Assume that the P_i's have no common zero in $\mathbf{C}^n$. Using Hilbert Nullstellensatz, deduce that the ideal of $\mathbf{Z}[X_1, \ldots, X_n]$ generated by the P_i's contains a nonzero integer m. For F a field of characteristic not dividing m, check that the P_i's have no common root in F^n.
`remark.` A spécial case (namely with a single polynomial $P(X) = X^2 - a$) is quoted by Serre in his *Course in arithmetic*, §4.4.

5 Solutions of some exercices

Solution to Exercise 2.
Let φ be the morphism of algebras $A_1[X_1, \ldots, X_n] \to A_2[y_1, \ldots, y_n]$ which maps X_i to y_i and whose restriction to A_1 is f. The kernel of φ is the set of polynomials P in $A_1[X_1, \ldots, X_n]$ such that the polynomial $Q \in A_2[X_1, \ldots, X_n]$, image of P by the extension of f to $A_1[X_1, \ldots, X_n] \to A_2[X_1, \ldots, X_n]$, satisfies

$$Q(y_1, \ldots, y_n) = 0.$$

The kernel of the morphism $\psi : A_1[X_1, \ldots, X_n] \to A_1[x_1, \ldots, x_n]$, which maps X_i to x_i and whose restriction to A_1 is the identity, is the set of polynomials P in $A_1[X_1, \ldots, X_n]$ such that $P(x_1, \ldots, x_n) = 0$. The result is that F exists if and only if $\ker \psi \subset \ker \varphi$.

□

Solution to Exercise 4.
See for instance [8], § 10.2.

□

Solution to Exercise 6.
See, for instance, [8] § 2.6. □

Solution to Exercise 8.

(a) The kernel of the endomorphism $x \mapsto x^2$ of the multiplicative group $F^\times$ is $\{\pm 1\}$, since q is odd this is a subgroup with 2 elements of $F^\times$, hence the image $\mathcal{C}$, which is the set of non–zero squares in F, has index 2 in $F^\times$: there are $(q-1)/2$ squares and $(q-1)/2$ nonsquares in $F^\times$. Each square is a root of $X^{(q-1)/2} - 1$, and therefore

$$X^{(q-1)/2} - 1 = \prod_{x \in \mathcal{C}} (X - x).$$

Since

$$\prod_{a \in F^\times} (X - a) = X^{q-1} - 1 = (X^{(q-1)/2} - 1)(X^{(q-1)/2} + 1),$$

we deduce

$$X^{(q-1)/2} + 1 = \prod_{x \in F^\times \setminus \mathcal{C}} (X - x).$$

(b) From (a) we deduce

$$X^{(p-1)/2} - 1 = \prod_{a \in \mathbf{F}_p,\, \left(\frac{a}{p}\right) = 1} (X - a)$$

and

$$X^{(p-1)/2} + 1 = \prod_{a \in \mathbf{F}_p,\, \left(\frac{a}{p}\right) = -1} (X - a).$$

It follows that for a in $\mathbf{F}_p$,

$$\left(\frac{a}{p}\right) = a^{(p-1)/2}.$$

□

Solution to Exercise 9**.**
Since 0 is a square, any square is the sum of two squares.

If F is a finite field of characteristic 2, the Frobenius $x \mapsto x^2$ is an automorphism of F, hence any element is a square in a unique way.

Assume F is a finite field with odd characteristic and with q elements. Consider the partition $F = Q \bigcup N$ where Q is the set of squares and N the set of non squares.

According to Exercise 8, the squares in F are the roots of

$$X(X^{(q-1)/2} - 1) = X^{(q+1)/2} - X,$$

hence Q has $(q+1)/2$ elements while N has $(q-1)/2$ elements.

Let $t \in F$. The set $t - Q$ has $(q+1)/2$ elements, and $(q+1)/2 > (q-1)/2$, therefore one at least of these elements, say $t - x$ with $x \in Q$, is not in N – hence it is in Q. Let $y = t - x$. We have written $t = x + y$ as a sum of two squares. □

Solution to Exercise 10**.**
In a field F with q elements, any element x satisfies $x^q = x$, hence $x^q - x + 1 \neq 0$. This proves that F is not algebraically closed. □

Solution to Exercise 13**.**
The kernel of the endomorphism $x \mapsto x^k$ of the multiplicative group $F^\times$ is the set of k–th roots of unity in F, the number of its elements is $\gcd(k, q-1)$, hence the number of elements in $\mathcal{C}_k$ is

$$\frac{q-1}{\gcd(k, q-1)}.$$

□

Solution to Exercise 20**.**
(a) Let $n = ms + r$ with $0 \leq r < m$ be the Euclidean division of n by m in $\mathbf{Z}$, with quotient s and remainder r. From

$$X^n - 1 = (X^{ms} - 1)X^r + X^r - 1$$

we deduce that

$$X^n - 1 = (X^m - 1)S + X^r - 1$$

is the Euclidean division of $X^n - 1$ by $X^m - 1$ in $\mathbf{Z}[X]$, with quotient

$$S(X) = \frac{X^{ms} - 1}{X^m - 1} X^r = X^{m(s-1)+r} + X^{m(s-2)+r} + \cdots + X^{m+r} + X^r$$

and remainder $X^r - 1$.
(b) For $n = ms + r$, writing

$$a^n - 1 = a^r(a^{ms} - 1) + a^r - 1,$$

we deduce that

$$\gcd(a^n - 1, a^m - 1) = \gcd(a^m - 1, a^r - 1).$$

The result follows by induction on $\max\{n, m\}$. □

Solution to Exercise 24**.**
(a) (See example 50).
(b) (See example 51).

(c) (See example 63).
(d) According to example 63, we have

$$\mathbf{F}_4 = \mathbf{F}_2[Y]/(Y^2 + Y + 1),$$

hence $\mathbf{F}_4 = \mathbf{F}_2(j)$ where $j^2 = j+1$. Over $\mathbf{F}_4 = \mathbf{F}_2(j)$, the polynomial X^2+X+j is irreducible. □

Solution to Exercise 25**.**
(a) Irreducible polynomials over $\mathbf{F}_2$:
degree 1: X, $X + 1$
degree 2: $X^2 + X + 1$ (see see Example 50)
degree 3: $X^3 + X + 1$ and $X^3 + X^2 + 1$ (see Example 51)
degree 4: $X^4 + X + 1$, $X^4 + X^3 + 1$, Φ_5 (see Example 63)
degree 5: there are six of them: write $P(0) \neq 0$, $P(1) \neq 0$ and omit

$$(X^2+X+1)(X^3+X+1) = X^5+X^4+1 \quad \text{and} \quad (X^2+X+1)(X^3+X^2+1) = X^5+X+1.$$

Remain:

$$X^2 + aX^4 + bX^3 + cX^2 + (a + b + c + 1)X + 1$$

with a, b, c in $\mathbf{F}_2$ omitting $(1, 0, 0)$ and $(0, 0, 0)$.
(b) Write $\mathbf{F}_4 = \{0, 1, j, j^2\}$. The four irreducible polynomials of degree 1 over $\mathbf{F}_4$ are X, $X - 1$, $X - j$, $X - j^2$. For the 6 irreducible polynomials of degree 2 over $\mathbf{F}_4$, see Exercise 67. □

Solution to Exercise 27.
a) Let $s : G \to G/N$ be the canonical surjective morphism of groups with kernel N. The restriction of s to H has kernel $H \cap N$ and image $s(H) = (H+N)/N$, hence

$$s(H) = \frac{H+N}{N} \simeq \frac{H}{H \cap N}.$$

Since $s(H)$ is a subgroup of G/N, its order, which is the index of $H \cap N$ in H, divides the order of G/N, which is the index of N in G.

If $H \cap N = \{1\}$, then the index of $H \cap N$ in H is the order of H.
(b) We apply (a) with G the Galois group of the extension $L/E_1 \cap E_2$, which is a finite abelian group, H the Galois group of L/E_1 and N the Galois group of L/E_2. The order of H is $[L : E_1]$ while the index of N in G is $[E_2 : E_1 \cap E_2]$. The conclusion follows from the remark that $[E_2 : E_1 \cap E_2]$ divides $[E_2 : K]$:

$$\begin{array}{ccccc} & & L & & \\ & H\,/ & & \backslash\, N & \\ E_1 & & G| & & E_2 \\ & \backslash & & / & \\ & & E_1 \cap E_2 & & \\ & & | & & \\ & & K & & \end{array}$$

c) Let $E_a = F(\alpha+\beta) \cap F(\alpha)$ and $E_b = F(\alpha+\beta) \cap F(\beta)$. We apply (b) with $L = F(\alpha,\beta)$, $K = F$, $E_1 = F(\alpha)$ or $F(\beta)$, $E_2 = F(\alpha+\beta)$:

$$\begin{array}{ccc} & F(\alpha,\beta) & \\ / & & \backslash \\ E_a & & F(\alpha+\beta) \\ \backslash & & / \\ & F & \end{array} \qquad\qquad \begin{array}{ccc} & F(\alpha,\beta) & \\ / & & \backslash \\ F(\alpha+\beta) & & E_b \\ \backslash & & / \\ & F & \end{array}$$

The first diagram shows that $[F(\alpha,\beta) : F(\alpha+\beta)]$ divides $[E_a : F] = a$, while the second diagram shows that $[F(\alpha,\beta) : F(\alpha+\beta)]$ divides $[E_b : F] = b$, hence $[F(\alpha,\beta) : F(\alpha+\beta)] = 1$ and therefore $F(\alpha,\beta) = F(\alpha+\beta)$. □

Solution to Exercise 33.
(a) The formula to be proved can be written

$$\Phi_{m_1}(X^{p^r}) = \Phi_m(X)\Phi_{m_1}(X^{p^{r-1}})$$

for $m = p^r m_1$ with $\gcd(p, m_1) = 1$. This formula follows by induction on m from

$$X^m - 1 = (X^{p^r})^{m_1} - 1 = \prod_{d|m_1} \Phi_d(X^{p^r})$$

and

$$X^m - 1 = \prod_{d|m} \Phi_d(X) = \prod_{k=0}^{r} \prod_{d|m_1} \Phi_{p^k d}(X).$$

(b) If m is odd, the map $\zeta \mapsto -\zeta$ is a bijective map from the set of m-th roots of unity to the set of $2m$-th roots of unity. Further, for $m \geq 3$, the number $\varphi(m)$ is even.

If m is odd and if ζ is a primitive $2m$-th root of unity, then $-\zeta$ is also a primitive $2m$-th root of unity and ζ^2 is a primitive m-th root of unity. The number of primitive $2m$-th roots of unity is therefore twice the number of primitive m-th roots of unity, which means $\varphi(2m) = 2\varphi(m)$, and the monic polynomials $\Phi_m(X^2)$ and $\Phi_{2m}(X)$ have the same (simple) roots, hence are the same.

□

Solution to Exercise 36. Write the decomposition of n into prime factors

$$n = p_1^{a_1} \cdots p_k^{a_k}.$$

We have

$$\frac{\varphi(n)}{n} = \frac{p_1}{p_1 - 1} \cdots \frac{p_k}{p_k - 1}.$$

Set

$$\lambda = 1 - \frac{\log 4}{\log 5},$$

so that

$$\frac{p_i}{p_i - 1} \leq \frac{5}{4} \leq p_i^{\lambda} \quad \text{for} \quad i \geq 3.$$

Thus

$$\frac{\varphi(n)}{n} \leq 3(p_3 \cdots p_k)^{\lambda} \leq 2.341(p_1 \cdots p_k)^{\lambda} \leq 2.341 n^{\lambda},$$

so that

$$n \leq \big(3.341\varphi(n)\big)^{1/(1-\lambda)} \leq 2.685\varphi(n)^{1.161}$$

for all $n \geq 1$.

`Remark`. It is known that for any $\epsilon > 0$, there exists an integer $n_0 > 0$ such that, for $n \geq n_0$,

$$n \leq (e^{\gamma} + \epsilon)\varphi(n) \log\log \varphi(n)$$

where γ is Euler's constant. Equivalently,

$$\varphi(n) \geq (e^{-\gamma} - \epsilon)\frac{n}{\log\log n}$$

for sufficiently large n. □

Solution to Exercise 40.
(a) Assume p does not divide m. We prove the relation in characteristic p:

$$\Phi_{p^r m}(X) = \Phi_m(X)^{\varphi(p^r)}$$

by induction on $p^r m$. We have

$$X^{p^r m} - 1 = (X^m - 1)^{p^r}. \tag{109}$$

Writing a divisor of $p^r m$ as $p^k d$ with d dividing m and $0 \leq k \leq r$, using the induction hypothesis and the equality

$$\sum_{k=0}^{r} \varphi(p^k) = p^r,$$

we see that the left hand side of (109) is

$$\begin{aligned}
\prod_{d|p^r m} \Phi_d(X) &= \prod_{k=0}^{r} \prod_{d|m} \Phi_{p^k d}(X) \\
&= \Phi_{p^r m}(X) \left(\prod_{k=0}^{r-1} \Phi_{m p^k}(X) \right) \left(\prod_{d|m, d \neq m} \prod_{k=0}^{r} \Phi_{p^k d}(X) \right) \\
&= \Phi_{p^r m}(X) \left(\prod_{k=0}^{r-1} \Phi_m(X)^{\varphi(p^k)} \right) \left(\prod_{d|m, d \neq m} \prod_{k=0}^{r} (\Phi_d(X))^{\varphi(p^r)} \right) \\
&= \Phi_{p^r m}(X) \Phi_m(X)^{p^{r-1}} \prod_{d|m, d \neq m} (\Phi_d(X))^{p^r}
\end{aligned}$$

while the right hand side of (109) is

$$\prod_{d|m} (\Phi_d(X))^{p^r}.$$

This completes the proof of (a)
(b) If $m = m_1 p^k$ with $k \geq 1$ and $\gcd(m_1, p) = 1$, then

$$\Phi_m(X) = \Phi_{m_1 p^k}(X) = \Phi_{m_1}(X)^{p^k - p^{k-1}},$$

$$\Phi_{p^r m}(X) = \Phi_{m_1 p^{r+k}}(X) = \Phi_{m_1}(X)^{p^{r+k} - p^{r+k-1}},$$

hence

$$\Phi_{p^r m}(X) = \Phi_m(X)^{p^r}.$$

□

Solution to Exercise 44**.**
(a) From (42) it follows that the number $N_2(n)$ of irreducible polynomials of

degree n over $\mathbf{F}_2$ satisfies the following relations.

$$\begin{aligned}
2^1 = N_2(1), &\quad \text{hence} \quad N_2(1) = 2.\\
2^2 = 4 = N_2(1) + 2N_2(2), &\quad \text{hence} \quad N_2(2) = 1.\\
2^3 = 8 = N_2(1) + 3N_2(3), &\quad \text{hence} \quad N_2(3) = 2.\\
2^4 = 16 = N_2(1) + 2N_2(2) + 4N_2(4), &\quad \text{hence} \quad N_2(4) = 3.\\
2^5 = 32 = N_2(1) + 5N_2(5), &\quad \text{hence} \quad N_2(5) = 6.\\
2^6 = 64 = N_2(1) + 2N_2(2) + 3N_2(3) + 6N_2(6), &\quad \text{hence} \quad N_2(6) = 9.
\end{aligned}$$

(b) and (c) The upper bound

$$N_q(n) \leq \frac{1}{n}(q^n - q)$$

for $n > 1$ can be checked as follows. On the one hand, each irreducible polynomial of degree n over $\mathbf{F}_q$ has n roots in $\mathbf{F}_{q^n}$. On the other hand, since $n > 1$, the number of elements in $\mathbf{F}_{q^n}$ having degree n over $\mathbf{F}_q$ is $\leq q^n - q$; each of these elements has n conjugates over $\mathbf{F}_q$. Therefore the number of roots in $\mathbf{F}_{q^n}$ of the irreducible polynomials of degree n over $\mathbf{F}_q$ is $\leq q^n - q$. It follows that the number of irreducible polynomials of degree n over $\mathbf{F}_q$ is $\leq (q^n - q)/n$.

On the other hand from (42) we deduce

$$\begin{aligned}
q^n - nN_q(n) &= \sum_{d|n, d<n} dN_q(d)\\
&\leq \sum_{d|n, d<n} q^d\\
&\leq \sum_{0 \leq k \leq n/2} q^k\\
&= \frac{q^{\lfloor n/2 \rfloor + 1} - 1}{q - 1}\\
&< q^{\lfloor n/2 \rfloor + 1}.
\end{aligned}$$

Hence

$$N_q(n) < \frac{q^n - q^{\lfloor n/2 \rfloor + 1}}{n}.$$

(See also [8], Theorem 19.10).

(d) As soon as

$$q^n \geq 4q^{n/2},$$

more than half of the elements α in $\mathbf{F}_q$ satisfy $\mathbf{F}_q = \mathbf{F}_p(\alpha)$.

(e) There are q^n monic polynomials of degree n in $\mathbf{F}_q[X]$. Since

$$\lim_{q^n \to \infty} \frac{nN_q(n)}{q^n} = 1,$$

the number $N_q(n)$ of monic irreducible polynomials of degree n in $\mathbf{F}_q[X]$ is asymptotically q^n/n.

□

Solution to Exercise 53.
From

$$3^5 = 243 = 22 \times 11 + 1$$

we deduce that the class of 3 has order 5 modulo 11. Hence Φ_{11}, which has degree $\varphi(11) = 10$, splits into two irreducible polynomials of degree 5 over $\mathbf{F}_3$:

$$\Phi_{11}(X) = f(X)g(X)$$

where

$$f(X) = X^5+X^4-X^3+X^2-1 \quad \text{and} \quad g(X) = X^5 f(1/X) = X^5-X^3+X^2-X-1.$$

□

Solution to Exercise 54.
The group $(\mathbf{Z}/23\mathbf{Z})^\times$ is cyclic of order 22, the elements have order 1, 2, 11 or 22. Clearly 2 is not of order 1 nor 2. Compute 2^{11} modulo 23:

$$2^6 = 64 \equiv -5 \pmod{23}, \quad 2^9 \equiv -40 \pmod{23}, \quad 2^{10} \equiv 12 \pmod{23},$$

hence $2^{11} \equiv 1 \pmod{23}$ and 2 has order 11 modulo 23. It follows that Φ_{23}, which has degree $\varphi(23) = 22$, is the product of two polynomials of degree 11 over $\mathbf{F}_2$.

□

Solution to Exercise 57.
The polynomial $\Phi_8(X) = X^4 + 1$ has no root in $\mathbf{Q}$, and is not the product of two degree 2 polynomials. Hence it is irreducible over $\mathbf{Q}$.

Over $\mathbf{F}_2$, $X^4 + 1 = (X + 1)^4$ is totally decomposed.

Let p be an odd prime. Over $\mathbf{F}_p$, Φ_8 splits into factors of all the same degree d, which is the order of p modulo 8.

For any odd prime p, the number $p^2 - 1 = (p - 1)(p + 1)$ is a multiple of 8 (each of $p - 1$ and $p + 1$ is even, one of them is divisible by 4). Hence $p^2 \equiv 1 \mod 8$, which proves that the order d of $p \mod 8$ is 1 or 2.

Notice that $d = 1$ if and only if $p \equiv 1 \mod 8$. Indeed, $\mathbf{F}_p^\times$ contains a subgroup of order 8 if and only 8 divides $p - 1$. Hence $d = 2$ for p congruent to 3, 5 or 7 modulo 8. □

Solution to Exercise 59**.**
The group $(\mathbf{Z}/15\mathbf{Z})^\times$ is a product $C_2 \times C_4$ of a cyclic group of order 2 by a cyclic group of order 4, hence there are 4 elements of order 4 (namely the classes of 2, 7, 8, 13) and 3 elements of order 2 (namely the classes of 4, 11 and 14).

Since the group $(\mathbf{Z}/15\mathbf{Z})^\times$ is not cyclic, Φ_{15} is always reducible over $\mathbf{F}_q$.

If $\gcd(15, q) = 1$, then Φ_{15} decomposes over $\mathbf{F}_q$ into a product of
• 8 factors of degree 1 if $q \equiv 1 \pmod{15}$,
• 4 factors of degree 2 if $q \equiv 4,\ 11,\ 14 \pmod{15}$,
• 2 factors of degree 4 if $q \equiv 2,\ 7,\ 8,\ 14 \pmod{15}$.

In characteristic 3, $\Phi_{15}(X) = \Phi_5(X)^2$. Recall Example 58. Since 3 has order 4 modulo 5, if $q = 3^r$, then over $\mathbf{F}_q$, the polynomial Φ_5
• splits into 4 linear factors if $r \equiv 0 \pmod 4$ (hence Φ_{15} splits completely),
• splits into 2 factors of degree 2 if $r \equiv 2 \pmod 4$ (hence Φ_{15} splits into 4 quadratic factors),
• is irreducible if $r \equiv 1$ or $3 \pmod 4$ (hence Φ_{15} splits into 2 factors of degree 4).

In characteristic 5, $\Phi_{15}(X) = \Phi_3(X)^4$. Assume $q = 5^r$. If r is odd, then over $\mathbf{F}_q$, the polynomial Φ_3 is irreducible and Φ_{15} splits into 4 quadratic factors, while if r is even, then over $\mathbf{F}_q$, the polynomial Φ_3 splits into two linear factors and Φ_{15} splits completely into 8 linear factors.

□

Solution to Exercise 60**.**
(a) The kernel of the homomorphism of multiplicative groups $f : \mathbf{F}_{q^2}^\times \longrightarrow \mathbf{F}_{q^2}^\times$ which maps x to x^{q-1} is $\mathbf{F}_q^\times$, it has $q - 1$ elements; the image of f is the set of roots of $X^{q+1} - 1$, it has $q + 1$ elements.
(b) Since the image of f has $q + 1$ elements, there exists $\gamma \in \mathbf{F}_{q^2}$ in the image of f, say $\gamma := \alpha^{q-1}$, which is not in $\mathbf{F}_q$. The two elements 1 and α^{q-1} are lineary independent over $\mathbf{F}_q$, which means (since $\alpha \neq 0$) that (α, α^q) are linearly independent over $\mathbf{F}_q$. □

Solution to Exercise 65**.**
Write $q = p^r$. If $q - 1$ is a prime number, then $q - 1$ is a Mersenne prime, the characteristic p is 2 and r is prime. Since $[\mathbf{F}_q : \mathbf{F}_2] = r$ is prime, any element in $\mathbf{F}_q \setminus \mathbf{F}_2$ is a generator of the extension $\mathbf{F}_q/\mathbf{F}_2$. Since $\mathbf{F}_q^\times$ is a cyclic group of prime order, any element in $\mathbf{F}_q \setminus \mathbf{F}_2$ is a generator of the cyclic group $\mathbf{F}_q^\times$.

Conversely, assume that any element α in $\mathbf{F}_q$ such that $\mathbf{F}_q = \mathbf{F}_p(\alpha)$ is a generator of the cyclic group $\mathbf{F}_q^\times$. Since $\varphi(p - 1) < p$, we have $r \geq 2$. The number of generators of the cyclic group $\mathbf{F}_q^\times$ is $\varphi(N)$ with $N = q - 1$. Using the notation and the results of Exercise 44, we deduce that the number of elements in $\mathbf{F}_q$ of degree r over $\mathbf{F}_p$ is $rN_p(r)$ and satisfies $rN_p(r) > N/2$. By assumption $rN_p(r) = \varphi(N)$, hence $\varphi(N) > N/2$. Therefore N is odd and consequently the characteristic p is 2.

If $N = 2^r - 1$ is not prime, then

$$\varphi(N) \leq N - \lfloor \sqrt{N} \rfloor.$$

Indeed, N has a prime factor $\leq \sqrt{N}$, hence there are at least $\lfloor \sqrt{N} \rfloor$ integers in $[1, N]$ which are not prime to N.

On the other hand, according to Exercise 44, the number of elements in $\mathbf{F}_{2^r}$ of degree r over $\mathbf{F}_2$ is $rN_2(r)$ and satisfies

$$rN_2(r) \geq 2^r - 2 \cdot 2^{r/2}.$$

Recall the assumption $rN_2(r) = \varphi(N)$. We do not yet deduce the desired contradiction, but we can improve one at least of these inequalities.

If r is odd, the solution of Exercise 44 provides a refinement of this last inequality, namely

$$rN_2(r) \geq 2^r - 2 \cdot 2^{r/3}.$$

If r is even, $r = 2k$, then $N = (2^k - 1)(2^k + 1)$ has at least one prime divisor $\leq \sqrt{2^k + 1}$ (notice that for $k \geq 3$ one at least of the two numbers $2^k - 1$, $2^k + 1$ is composite). In this case

$$\varphi(N) \leq N - \lfloor \sqrt[4]{N} + 1 \rfloor.$$

These estimates are sufficient to complete the proof. □

Solution to Exercise 66**.**
Let q be the number of elements in F and n the degree of the extension E/F. Hence the field E has q^n elements. We have

$$\mathrm{N}_{E/F}(\alpha) = \alpha^{(q^n-1)/(q-1)}.$$

If $\mathrm{N}_{E/F}(\alpha)$ has order $< q-1$ in $F^\times$, then there exists an integer ℓ with $1 \leq \ell < q-1$ such that $\mathrm{N}_{E/F}(\alpha)^\ell = 1$, hence $\alpha^{(q^n-1)\ell/(q-1)} = 1$. Since

$$0 < \frac{(q^n - 1)\ell}{q - 1} < q^n - 1,$$

it follows that α has order $< q^n - 1$ in $E^\times$. □

Solution to Exercise 67**.**
Write $\mathbf{F}_4 = \{0, 1, j, j^2\}$ with $j^2 + j + 1 = 0$. There 16 elements in $\mathbf{F}_{16}$, two of degree 1 over $\mathbf{F}_2$ (the elements of $\mathbf{F}_2$), two of degree 2 (the elements of $\mathbf{F}_4 \setminus \mathbf{F}_2$), and 12 of degree 4 (the elements of $\mathbf{F}_{16} \setminus \mathbf{F}_4$). In the cyclic group $\mathbf{F}_{16}^\times$ of order 15 there are $\varphi(15) = 6$ elements of order 15, $\varphi(5) = 4$ elements of order 5 (namely the roots of Φ_5), 2 elements of order 3, namely j and j^2.

The 12 elements of $\mathbf{F}_{16}$ of degree 4 over $\mathbf{F}_2$ have degree 2 over $\mathbf{F}_4$. Among them, there are 8 elements of order 15 and 4 elements of order 5 in the group $\mathbf{F}_{16}^\times$. The 4 elements of order 5 are the roots of Φ_5 which is irreducible over $\mathbf{F}_2$

and which splits into 2 quadratic factors over $\mathbf{F}_4$. The 6 irreducible quadratic polynomials of $\mathbf{F}_4[X]$ come in pairs of conjugate polynomials over $\mathbf{F}_2$ (notice that Frob_2 permutes j and j^2):

$$\begin{aligned} &X^2+jX+1, \quad X^2+j^2+1\\ &X^2+X+j, \quad X^2+X+j^2,\\ &X^2+jX+j, \quad X^2+j^2X+j^2. \end{aligned}$$

Notice that

$$(A+jB)(A+j^2B) = A^2+AB+B^2,$$

hence

$$\begin{aligned} &(X^2+jX+1)(X^2+j^2+1) = X^4+X^3+X^2+X+1 = \Phi_5(X),\\ &(X^2+X+j)(X^2+X+j^2) = X^4+X+1,\\ &(X^2+jX+j)(X^2+j^2X+j^2) = X^4+X^3+1. \end{aligned}$$

These products are the three irreducible polynomials of degree 4 over $\mathbf{F}_2$.

Let α be a root of X^2+X+j. The other is α^4.

Taking the conjugate over $\mathbf{F}_2$, we deduce that the roots of X^2+X+j^2 are α^2 and α^6. The roots of $X^2+j^2X+j^2$ are α^{-1} and α^{-4}. Again, taking the conjugate over $\mathbf{F}_2$, we deduce that the roots of X^2+jX+j are α^{-2} and α^{-6}

The 4 elements of order 5 are α^3, α^{12} (they are conjugate) and α^6, α^9 (they are conjugate).

We have

$$\alpha^2 = \alpha+j, \quad \alpha^3 = \alpha+j+j\alpha, \quad \alpha^6 = j\alpha,$$

hence α^3 and α^{12} are the roots of X^2+j^2X+1, while α^6, α^9 are the roots of X^2+jX+1. □

Solution to Exercise 68**.**

(a) See Example 55.

(b) This is a special case of Exercise 66. Indeed, The norm over $\mathbf{F}_q$ of $a+ib \in \mathbf{F}_q(i)$ is

$$a^2+b^2 = (a+ib)(a-ib) = (a+ib)^{p+1},$$

hence if $a+ib$ is a primitive root in $\mathbf{F}_{p^2}$ then a^2+b^2 is a primitive root in $\mathbf{F}_p$.

Conversely, assume that a^2+b^2 has order $p-1$ in the multiplicative group $\mathbf{F}_p^\times$. If $(a+ib)^m = 1$, then $(a-ib)^m = 1$ and $(a^2+b^2)^m = 1$, therefore $p-1$ divides m, which means that the order of $a+ib$ is a multiple of $p-1$.

Also, we have

$$(a^2+b^2)^{(p-1)/2} = (a+ib)^{(p-1)(p+1)/2} = -1,$$

hence the order of $a+ib$ does not divide $(p^2-1)/2$.

(c) Assume now that p is a Mersenne prime. Using the fact that $p+1$ is a power of 2, we deduce that the only multiple of $p-1$ which divides p^2-1 but does not divide $(p^2-1)/2$ is p^2-1 itself. □

Solution to Exercise 83**.**
(a) The divisors of 12 are $1, 2, 3, 4, 6$ and 12, hence,

$$X^{12} - 1 = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X)$$

with

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1,$$
$$\Phi_4(X) = \Phi_2(X^2) = X^2 + 1, \quad \Phi_6(X) = \Phi_3(-X) = X^2 - X + 1,$$

and

$$\Phi_{12} = \Phi_6(X^2) = X^4 - X^2 + 1.$$

(b) According to Theorem 45, the polynomial $\Phi_n(X)$ splits in the finite field with q elements into a product of irreducible polynomials, all of the same degree d, where d is the order of q modulo n. We have

$$5 \equiv 1 \bmod 1, \quad 5 \equiv 1 \bmod 2, \quad 5 \equiv 1 \bmod 4,$$

$$5 \not\equiv 1 \bmod 3, \quad 5 \not\equiv 1 \bmod 6, \quad 5 \not\equiv 1 \bmod 12,$$
$$5^2 \equiv 1 \bmod 3, \quad 5^2 \equiv 1 \bmod 6, \quad 5^2 \equiv 1 \bmod 12,$$

which means that 5 has order 1 modulo 1, 2 and 4, order 2 modulo 3, 6 and 12. Therefore, in $\mathbf{F}_5[X]$, the polynomial $\Phi_4(X)$ is product of two linear polynomials:

$$X^2 + 1 = (X + 2)(X + 3) \quad \text{in } \mathbf{F}_5[X],$$

$\Phi_3(X)$, $\Phi_6(X)$ are irreducible and $\Phi_{12}(X)$ is product of two irreducible quadratic factors:

$$X^4 - X^2 + 1 = (X^2 + 2X - 1)(X^2 + 3X - 1).$$

Hence, in $\mathbf{F}_5[X]$, the polynomial $X^{12} - 1$ is a product of 6 linear polynomials and three irreducible quadratic polynomials.
(c) Let K be the splitting field over $\mathbf{F}_5$ of $X^{12} - 1$. The root of any of the three irreducible quadratic factors in $\mathbf{F}_5$ of $X^{12} - 1$ generated over $\mathbf{F}_5$ the unic quadratic extension of $\mathbf{F}_5$ contained in K. Hence, $[K : \mathbf{F}_5] = 2$ and K has 25 elements.

(d) Over $\mathbf{F}_2$, the polynomial $X^2 + X + 1$ is irreducible and

$$X^{12} - 1 = (X^3 - 1)^4 = (X - 1)^4(X^2 + X + 1)^4$$

is the product of four linear polynomials and four irreducible quadratic polynomials.

Over $\mathbf{F}_3$, the polynomial $X^2 + 1$ is irreducible and

$$X^{12} - 1 = (X^4 - 1)^3 = (X - 1)^3(X + 1)^3(X^2 + 1)^3$$

is the product of six linear polynomials and three irreducible quadratic polynomials.

Assume now $p \geq 5$. Since p does not divide 12, the polynomial $X^{12}-1$ has no multiple factor. There are always two degree 1 factors, namely $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$. For each of the other factors $\Phi_d(X)$ with d a divisor of 12 and $d > 2$ (hence, $d = 3$, 4, 6 or 12), if m is the order of p modulo d, then Φ_d splits over $\mathbf{F}_p$ into a product of polynomials, all of degree m. Here is the result:

p modulo 12	1	5	7	11
p modulo 3	1	-1	1	-1
p modulo 4	1	1	-1	-1
p modulo 6	1	-1	1	-1
order of p modulo 12	1	2	2	2
order of p modulo 3	1	2	1	2
order of p modulo 4	1	1	2	2
order of p modulo 6	1	2	1	2

Hence, $X^{12} - 1$ is product of

- 12 linear factors (it splits completely over $\mathbf{F}_p$) if $p \equiv 1 \bmod 12$,
- 4 linear factors and 4 irreducible quadratic factors if $p \equiv 5 \bmod 12$,
- 6 linear factors and 3 irreducible quadratic factors if $p \equiv 7 \bmod 12$,
- 2 linear factors and 5 irreducible quadratic factors if $p \equiv 11 \bmod 12$. □

Solution to Exercise 84**.**
(a) The order of 2 and of 3 modulo 5 is $4 = \varphi(5)$, hence the cyclotomic polynomial

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$$

is irreducible over $\mathbf{F}_2$ and over $\mathbf{F}_3$. (See Example 58).

The order of 2 modulo 7 is 3, hence Φ_7 splits into a product of two irreducible polynomials of degree 3 over $\mathbf{F}_2$.

The order of 3 modulo 7 is $6 = \varphi(7)$, hence Φ_7 is irreducible over $\mathbf{F}_3$.

The order of 2 modulo 11 is $10 = \varphi(11)$, hence Φ_{11} is irreducible over $\mathbf{F}_2$.

The order of 3 modulo 11 is 5, hence Φ_{11} splits into a product of two irreducible polynomials of degree 5 over $\mathbf{F}_2$.
(b) The order of 2 modulo 15 is 4, the degree of Φ_{15} is $\varphi(15) = 8$, hence Φ_{15} splits into a product of two irreducible polynomials of degree 4 over $\mathbf{F}_2$:

$$\Phi_{15}(X) = (X^4 + X^3 + 1)(X^4 + X + 1).$$

(See example 63).
(c) The polynomial $X^4 + X + 1$ is irreducible over $\mathbf{F}_2$, over $\mathbf{F}_4 = \{0, 1, j, j^2\}$ with $1 + j + j^2 = 0$ it splits into two irreducible quadratic factors

$$X^4 + X + 1 = (X^2 + X + j)(X^2 + X + j^2).$$

(See exercise 67). Since $[\mathbf{F}_8 : \mathbf{F}_2] = 3$ and $\gcd(2, 3) = 1$, it follows that X^4+X+1 is irreducible over $\mathbf{F}_8$.

(d) The polynomials $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$ are irreducible over any field. The polynomial $\Phi_4(X) = X^2 + 1$ splits into $(X+1)^2$ in characteristic 2.

Let Φ_n be a cyclotomic polynomial which is irreducible over $\mathbf{F}_q$ where $q \in \{1,\ 2,\ 4,\ 8,\ 16\}$. Then the class of q modulo n is a generator of $(\mathbf{Z}/n\mathbf{Z})^\times$, in particular this group is cyclic, hence (exercise 4) $n \in \{2, 4, p^s, p^{2s}\}$ where p is an odd prime and $s \geq 1$. Since $\Phi_{2p^s}(X) = \Phi_{p^s}(-X)$ (see exercise 33), it only remains to use the fact that for $n = p^s$ with p odd prime and $s \geq 1$,

• Φ_n is irreducible over $\mathbf{F}_2$ if and only if 2 is a generator of the cyclic group $(\mathbf{Z}/n\mathbf{Z})^\times$,

• Φ_n is irreducible over $\mathbf{F}_4$ if and only if 4 is a generator of the cyclic group $(\mathbf{Z}/n\mathbf{Z})^\times$,

• Φ_n is irreducible over $\mathbf{F}_8$ if and only if 8 is a generator of the cyclic group $(\mathbf{Z}/n\mathbf{Z})^\times$,

• Φ_n is irreducible over $\mathbf{F}_{16}$ if and only if 16 is a generator of the cyclic group $(\mathbf{Z}/n\mathbf{Z})^\times$.

The polynomial $\Phi_3(X) = 1 + X + X^2$ is irreducible over $\mathbf{F}_2$ and $\mathbf{F}_8$, it splits into linear factors over $\mathbf{F}_4$ hence also over $\mathbf{F}_{16}$.

The polynomial Φ_5 is irreducible over $\mathbf{F}_2$ hence over $\mathbf{F}_8$ (it has degree 4 prime to $[\mathbf{F}_8 : \mathbf{F}_2] = 3$), it is reducible over $\mathbf{F}_4$ (since 4 has order 2 modulo 5), hence also over $\mathbf{F}_{16}$.

The polynomial Φ_7 is reducible over $\mathbf{F}_2$ (since 2 has order 3 modulo 7), hence also over $\mathbf{F}_4$, $\mathbf{F}_8$ and $\mathbf{F}_{16}$.

The polynomial Φ_{11} is irreducible over $\mathbf{F}_2 \ldots$

$n = p^s$, $\varphi(n) = p^{s-1}(p-1)$, $(\mathbf{Z}/p^s\mathbf{Z})^\times$ is a product of a cyclic group of order p^{s-1} and a cyclic group of order $p-1$. If Φ_n is irreducible over $\mathbf{F}_2$, then the class of 2 modulo p has order $p-1$, hence $2^{(p-1)/2} \equiv -1 \pmod{p}$ which means that the Legendre symbol $\left(\frac{2}{p}\right)$ is -1, which means $p \equiv 3$ or $5 \pmod{8}$.

It follows that for $p \equiv 1$ or $-1 \pmod{8}$, Φ_p is reducible in characteristic 2.

Let ζ be a primitive p-th root of unity in characteristic 2.

If $p \equiv 5 \pmod{8}$, then $p \equiv 1 \pmod{4}$, Φ_p is reducible over $\mathbf{F}_4$.

If $p \equiv 3 \pmod{8}$, then Φ_p is irreducible over $\mathbf{F}_4$.

Over $\mathbf{F}_8$, the condition is 3 divides $(p-1)/2$, hence $p \equiv 1 \pmod{6}$.

Over $\mathbf{F}_{16}$, the condition is 4 divides $(p-1)/2$, hence $p \equiv 1 \pmod{8}$. Hence Πhi_n is always reducible over $\mathbf{F}_{16}$.

□

Solution to Exercise 85**.**

Denote by $\mathcal{N}_q(n)$ the number of squarefree monic polynomials in $\mathbf{F}_q[X]$ of degree n. Clearly $\mathcal{N}_q(0) = 1$ and $\mathcal{N}_q(1) = q$.

Any monic polynomial in $\mathbf{F}_q[X]$ of degree n can be written in a unique way A^2B, where A is a monic polynomial of degree, say, d, with $0 \leq d \leq n/2$ and B is a monic squarefree polynomial of degree $n - 2d$. This yields a partition of

the set of monic polynomials of degree n, which implies

$$q^n = \sum_{0 \le d \le n/2} q^d \mathcal{N}_q(n-2d)$$
$$= \mathcal{N}_q(n) + q\mathcal{N}_q(n-2) + q^2\mathcal{N}_q(n-4) + \cdots + \begin{cases} q^{n/2}\mathcal{N}_q(0) & \text{if } n \text{ is even,} \\ q^{(n-1)/2}\mathcal{N}_q(1) & \text{if } n \text{ is odd.} \end{cases}$$

The formula $\mathcal{N}_q(n) = q^n - q^{n-1}$ for $n \ge 2$ follows by induction on n (telescoping sum). □

Solution to Exercise 86**.**
Since $728 = 3^6 - 1$, the order of 3 modulo 728 is 6. We also check

$$728 = 2^3 \cdot 7 \cdot 13 \quad \text{and therefore} \quad \varphi(728) = 2^5 \cdot 3^2 = 48 \cdot 6.$$

Hence, over the field $\mathbf{F}_3$, the cyclotomic polynomial Φ_{728} splits into a product of 48 irreducible factors, each of which has degree 6. □

Solution to Exercise 87**.**
The polynomial $X^3 + X + 1$ is irreducible over $\mathbf{F}_5$. Let α be a root of this polynomial in $\mathbf{F}_{5^3}$. One checks

$$\alpha^5 = -\alpha^2 + \alpha + 1, \quad \alpha^{15} = \alpha^2 - \alpha - 2, \quad \alpha^{30} = \alpha^2 + 1,$$

$$\alpha^{31} = -1, \quad (2\alpha)^{31} = -2, \quad (2\alpha)^{62} = -1.$$

It follows that 2α has order $124 = 5^3 - 1$, hence is a generator of the cyclic group $\mathbf{F}_{5^3}^\times$.

□

Solution to Exercise 88**.**
(a) If $\zeta \in K$ satisfies $\zeta^{q-1} = -1$, then $\zeta^q = -\zeta$ and $(\zeta^2)^q = (\zeta^q)^2 = \zeta^2$, hence $\zeta^2 \in \mathbf{F}_q^\times$.
(b) Assume first $p = 2$. Then

$$X^{2q-1} - X = X(X^{q-1} - 1)^2$$

splits into $2q - 1$ linear factors (degree 1) in $\mathbf{F}_q$.

Next assume q is odd. According to (a), the polynomial $X^{q-1} + 1$ has no root in $\mathbf{F}_q$, but it splits into linear factors in $\mathbf{F}_{q^2}$. Hence we have

$$X^{2q-1} - X = X(X^{q-1} - 1)(X^{q-1} + 1),$$

where $X(X^{q-1} - 1)$ is a product of q linear factors in $\mathbf{F}_q$, while $X^{q-1} + 1$ is a product of $(q-1)/2$ quadratic factors in $\mathbf{F}_q$. □

Solution to Exercise 89**.** Let p be the characteristic of F and $q = p^r$ the number of elements of F. Denote by σ_n the map $x \mapsto x^n$ from F to F.

If $n \equiv p^\ell \pmod{(q-1)}$ for some ℓ with $0 \leq \ell \leq r-1$, then for $x \in F^\times$ we have $\sigma_n(x) = \mathrm{Frob}_p^\ell(x)$, hence $\sigma_n = \mathrm{Frob}_p^\ell$, which is an automorphism of F.

Conversely, assume σ_n is an automorphism of F. Hence σ is an element of the Galois group of F over F_p, which means that there exist ℓ with $0 \leq \ell \leq r-1$ such that $\sigma = \mathrm{Frob}_p^\ell$. Let m be the class of n modulo $(q-1)$: hence $0 \leq m \leq q-2$ and $m - n$ is a multiple of $q-1$. Therefore $\sigma_n = \sigma_m$, where σ_m is the map $x \mapsto x^m$ from F to F. From $x^{p^\ell} = x^m$ for all $x \in F$ we deduce that the polynomial $X^q - X$ divides $X^{p^\ell} - X^m$. However $p^\ell < q$ and $m < q$, hence $m = p^\ell$.

Therefore the set of n such that σ_n is an automorphism of F is the set of integers congruent to a power of p modulo $q-1$.

□

Solution to Exercise 90**.**
(a) Since q divides $2^p - 1$, it follows that q is odd and that the order of the class of 2 in $(\mathbf{Z}/q\mathbf{Z})^\times$ is p, hence p divides $q-1$.
(b) Since q divides $2^{2^n} + 1$, it follows that q is odd and that the order of the class of 2 in $(\mathbf{Z}/q\mathbf{Z})^\times$ is 2^{n+1}, hence 2^{n+1} divides $q-1$. □

Solution to Exercise 91**.**
Since $a^p \equiv a \bmod p$, if $f(X) = (X^p - X)g(X) + ph(X)$, then, for all $a \in \mathbf{Z}$, the number p divides $f(a)$.

Conversely, assume that for any $a \in \mathbf{Z}$, the number p divides $f(a)$. Divide the polynomial f by $X^p - X$ in $\mathbf{Z}[X]$:

$$f(X) = (X^p - X)g(X) + r(X),$$

with g and r in $\mathbf{Z}[X]$, and r either zero, or else of degree $< p$. Then $r(a) \equiv 0 \bmod p$ for all $a \in \mathbf{Z}$, hence, the image of r in $\mathbf{F}_p[X]$ is zero. This means that there exists $h \in \mathbf{Z}[X]$ such that $r = ph$.

One can also argue as follows: when K is a field of characteristic p, we have

$$X^p - X = \prod_{\alpha \in \mathbf{F}_p} (X - \alpha),$$

hence, for $F \in K[X]$, the condition
(i)' For all $a \in \mathbf{F}_p$, $F(a) = 0$
is equivalent to
(ii)' There exists a polynomial $G \in \mathbf{F}_p[X]$ such that $F(X) = (X^p - X)G(X)$.
The statement of the exercise is a reformulation of this equivalence (take $K = \mathbf{F}_p$, and F, G are the reductions modulo p of f and g). □

Solution to Exercise 92**.**

We show that the kernel of f has p elements, which are the classes modulo p^2 of the integers $\equiv 1 \pmod{p^2}$, while the image of f has $p-1$ elements, which are the roots of $X^{p-1}-1$ in $(\mathbf{Z}/p^2\mathbf{Z})^\times$.

For $p=2$, we have $(\mathbf{Z}/4\mathbf{Z})^\times = \{1,-1\}$, the kernel of the homomorphism $f : x \mapsto x^2$ of this group is $(\mathbf{Z}/4\mathbf{Z})^\times$ and has two elements, the image of f is $\{1\}$, which is the set of roots of $X-1$, and has one elements,

Assume now that p is odd. Since $p^2\mathbf{Z} \subset p\mathbf{Z}$, the canonical surjective homomorphism $\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ factors as $\mathbf{Z} \to \mathbf{Z}/p^2\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$:

$$\begin{array}{ccc} \mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z} \\ \downarrow & \nearrow \varphi & \\ \mathbf{Z}/p^2\mathbf{Z} & & \end{array}$$

Let $\phi : (\mathbf{Z}/p^2\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$ be the restriction of φ to $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Since $(1+pt)^p \equiv 1 \pmod{p^2}$, any $x \in \ker\phi$ satisfies $x^p = 1$, and there are p such elements, namely the classes modulo p^2 of

$$1, 1+p, \ldots, 1+(p-1)p.$$

It follows that $\ker f$ has p elements, and therefore, since $(\mathbf{Z}/p^2\mathbf{Z})^\times$ has $p(p-1)$ elements, $\mathrm{Im}f$ has $p-1$ elements. Further, any element $y = x^p$ in the image of f satisfies $y^{p-1} = 1$, hence $\mathrm{Im}f$ is the set of roots of $X^{p-1}-1$. □

Solution to Exercise 93**.**

(a) Let $f \in \mathbf{F}_q[X]$ be the minimal polynomial of A over $\mathbf{F}_q$. The degree of f is at most n. The subring $\mathbf{F}_q[A]$ of $\mathrm{Mat}_{n\times n}(\mathbf{F}_q)$ generated by A is $\mathbf{F}_q[X]/(f)$. Let G be the subgroup of $\mathbf{F}_q[A]^\times$ generated by the class of A modulo f. The order of G divides the order of $\mathbf{F}_q[A]^\times$, and the order of $\mathbf{F}_q[A]^\times$ is at most q^n-1.

Take for instance $n=q=2$. Over $\mathbf{F}_2$, the 2×2 matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has order 2 which does not divide $2^n-1=3$.

(b) If A has order q^n-1, then (with the above notations) the group $G = \mathbf{F}_q[A]^\times$ has q^n-1 elements, hence $\mathbf{F}_q[A]$ is a field with q^n elements and A is a generator of G. Hence $(i) \Rightarrow (ii)$.

If $\mathbf{F}_q[A]$ is a field with q^n elements and A is a primitive element in this field, then the characteristic polynomial of A is a primitive polynomial. Hence $(ii) \Rightarrow (iii)$.

If the characteristic polynomial of A is a primitive polynomial, since it has degree n, it is the minimal polynomial f of A; the class of X in $\mathbf{F}_q[X]/(f)$ is a generator of the cyclic group $\mathbf{F}_q[A]^\times$, hence $\mathbf{F}_q[A]$ is a field with q^n elements and A has order q^n-1. Hence $(iii) \Rightarrow (i)$. □

Solution to Exercise 94**.**
Notice first that if there is a domain A such that $A^\times$ has order m, then the same is true for other domains like $A[X]$ - hence there is not unicity.

Also, if $A^\times$ is a finite group, then it is cyclic (being a finite subgroup of the multiplicative group of the quotient field of A).

The answer is yes for $m = p^r - 1$, hence for $m = 1, 2, 3, 4, 6, 7, 8, 10$, by taking for A the field with p^m elements. Let us show that the answer is no for $m = 5, 9$ and 11.

Assume $A^\times$ has order m with $m \in \{5, 9, 11\}$. Since m is odd, if follows that -1, which is a unit, cannot have order 2, and therefore $-1 = 1$, which means that A has characteristic 2.

The ring A contains the m–th roots of unity, hence contains $\mathbf{F}_2(\zeta)$ where ζ is a primitive m–th root of unity. The degree d of ζ is the order of 2 modulo m, hence $d = 4$ for $m = 5$, $d = 6$ for $m = 9$ and $d = 10$ for $m = 11$. Now $A^\times$ contains $\mathbf{F}_2(\zeta)^\times$ which is a group having $2^d > m$ elements. This is a contradiction.

□

Solution to Exercise 95**.**
(a) Two conjugate elements α and $\sigma(\alpha)$ have the same order, since $\alpha^m = 1$ if and only if $\sigma(\alpha)^m = 1$.
(b) Let α be a root of f. Since α has order $p(f)$ in the multiplicative group $\mathbf{F}_q(\alpha)^\times$ we have

$$p(f)|\ell \Longleftrightarrow \alpha^\ell = 1 \Longleftrightarrow f(X)|X^\ell - 1.$$

(c) The n conjugates of a root α of f over $\mathbf{F}_q$ are its images under the iterated Frobenius $x \mapsto x^q$, which is the generator of the cyclic Galois group of $\mathbf{F}_q(\alpha)/\mathbf{F}_q$. From $\alpha^{q^n} = \alpha$, we deduce that f divides the polynomial $X^{q^n} - X$ (see also Theorem 41). Since $f(X) \neq X$ we deduce $\alpha \neq 0$, hence, f divides the polynomial $X^{q^n-1} - 1$. As we have seen in question (b), it implies that $p(f)$ divides $q^n - 1$. The fact that the characteristic p does not divide $p(f)$ is then obvious.
(d) An irreducible monic polynomial $f \in \mathbf{F}_q[X]$ is primitive if and only if any root α of f in $\overline{\mathbf{F}}_p$ is a generator of the cyclic group $\mathbf{F}_q(\alpha)^\times$.
(e) Here is the answer:

q	d	$f(X)$	$p(f)$	primitive
2	2	$X^2 + X + 1$	3	yes
2	3	$X^3 + X + 1$	7	yes
2	3	$X^3 + X^2 + 1$	7	yes
2	4	$X^4 + X^3 + 1$	15	yes
2	4	$X^4 + X + 1$	15	yes
2	4	$X^4 + X^3 + X^2 + X + 1$	5	no
3	2	$X^2 + 1$	4	no
3	2	$X^2 + X - 1$	8	yes
3	2	$X^2 - X - 1$	8	yes

(f) The two irreducible polynomials of period 15 over $\mathbf{F}_2$ are the two factors X^4+X^3+1 and X^4+X+1 of Φ_{15}. The only irreducible polynomial of period 5 over $\mathbf{F}_2$ is $\Phi_5(X) = X^4+X^3+X^2+X+1$.

□

Solution to Exercise 96**.**
If $\ell = 2$ and p is odd, the assumption that a is not a square in $\mathbf{F}_p$ implies that $X^2 - a$ is irreducible over $\mathbf{F}_p$.

If ℓ is odd and $p = 2$, then for any $a \in \mathbf{F}_2$ the polynomial $X^\ell - a$ is reducible over $\mathbf{F}_2$.

If $p = \ell$, since the Frobenius $x \mapsto x^p$ is an automorphism of $\mathbf{F}_p$, any element in $\mathbf{F}_p$ is a p-th power and again the result is trivial.

Assume now that ℓ and p are distinct odd primes. Let ζ be an element of order $p-1$ in the multiplicative group $\mathbf{F}_p^\times$. If ℓ does not divide $p-1$, then ζ is a ℓ-th power (if m is the inverse of ℓ in the group $(\mathbf{Z}/(p-1)\mathbf{Z})^\times$, then $\zeta = \gamma^\ell$ with $\gamma = \zeta^m$), and in this case any element in $\mathbf{F}_p$ is a ℓ-th power. Therefore we need to consider only the prime numbers ℓ which divide $p-1$. In this case the ℓ–th roots of unity are in $\mathbf{F}_p$. Let $\zeta \in \mathbf{F}_p$ be a primitive ℓ-th root of unity. Let γ be a root of the polynomial $X^\ell - a$ in an extension of $\mathbf{F}_p$ and let $E = \mathbf{F}_p(\gamma)$. Since a is not an ℓ–th power in $\mathbf{F}_p$, we have $E \neq \mathbf{F}_p$. Also,

$$X^\ell - a = \prod_{j=0}^{\ell-1}(X - \zeta^j\gamma).$$

For $0 \leq j \leq \ell-1$, we have $\mathbf{F}_p(\gamma) = \mathbf{F}_p(\gamma\zeta^j)$, hence all $\gamma\zeta^j$ have the same degree $d \geq 2$ over $\mathbf{F}_p$, hence this degree divides ℓ. Given that ℓ is prime, we deduce $d = \ell$. □

Solution to Exercise 97**.**
Let α be a root in an extension of $\mathbf{F}_p$. Since $\alpha^p \neq \alpha$, we have $\alpha \notin \mathbf{F}_p$. The conjugates of α are α^{p^k} for $k = 0, \ldots, d-1$ where d, the degree of α over $\mathbf{F}_p$, is the least integer such that $\alpha^{p^d} = 1$. We have

$$\alpha^{p^k} - \alpha^{p^{k-1}} = u$$

for any $k \geq 1$. Hence

$$\alpha^{p^k} - \alpha = ku$$

and d is the least integer such that $du = 0$, which is $d = p$. □

Solution to Exercise 98**.**
The division of $(X+1)^k$ by $f(X) = X^3 + X + 1$ in $\mathbf{F}_2[X]$ is given by

$$\begin{aligned}
X+1 &= 0f + X + 1\\
(X+1)^2 &= 0f + X^2 + 1\\
(X+1)^3 &= f + X\\
(X+1)^4 &= Xf + X^2 + X + 1\\
(X+1)^5 &= (X^2+1)f + X^2 + X\\
(X+1)^6 &= (X^3 + X + 1)f + X^2\\
(X+1)^7 &= (X^4 + X^2 + X + 1)f,
\end{aligned}$$

hence the least integer k such that $(X+1)^k$ is multiple of f is $k = 7$.

Let $f \in \mathbf{F}_p[X]$ of degree n with $f(0) \neq 0$. For $1 \leq \ell \leq p^n$, write

$$X^\ell - 1 = f(X)Q_\ell(X) + R_\ell$$

with R_ℓ of degree $< n$. There are p^n polynomials of degree $< n$ over $\mathbf{F}_p$. If the R_ℓ are all distinct, one of them is 0, and then f divides the corresponding $X^\ell - 1$. If two of the R_ℓ are the same, say $R_\ell = R_k$ with $1 \leq \ell < k \leq p^n$, then $X^k - X^\ell = (X^{k-\ell} - 1)X^\ell$ divides f, and since X does not divide f, we deduce that $X^{k-\ell} - 1$ divides f while we have $1 \leq k - \ell \leq p^n - 1$.

The only case where this proof does not yield an exponent $< p^n$ is when the only ℓ where R_ℓ is 0 is p^n (and all the other R_ℓ are pairwise distinct). But in this case $X^{p^n} - 1 = (X-1)^{p^n}$ divides f, hence $f(X) = (X-1)^n$, but since $n \leq p^{n-1}$ it follows that $X^{p^{n-1}} - 1$ divides f. (So this case never happens). □

Solution to Exercise 99**.**
(a) Let x be a root of $X^{p-1} - u$ in an extension of $\mathbf{F}_p$. Then

$$x^{p^r} = u^r x$$

for all $r \geq 0$. Since u has order m in $\mathbf{F}_p^\times$, the least r such that $x^{p^r} = x$ is $r = m$. Since $k = (p-1)/m$, the orbit of x under the iterated of Frob_p has m elements, hence (Theorem 28) x has degree m over $\mathbf{F}_p$. Since all roots of $X^{p-1} - u$ have the same degree m over $\mathbf{F}_p$, in the decomposition of the polynomial $X^{p-1} - u$ into irreducible polynomials over $\mathbf{F}_p$, all factors have degree m.
(b) The multiplicative group H generated by u is the unique subgroup of $\mathbf{F}_p^\times$ of order m. The morphism

$$\begin{array}{ccc} \mathbf{F}_p^\times & \to & H \\ x & \mapsto & x^{(p-1)/m} \end{array}$$

is surjective, its kernel has $(p-1)/m$ elements, say $v_1, \ldots, v_k$, which are the solutions in $\mathbf{F}_p^\times$ of $v_i^k = u$.
(c) Since $X^m - v_i \in \mathbf{F}_p[X]$, we deduce that

$$X^{p-1} - u = \prod_{i=1}^{k} (X^m - v_i)$$

is the decomposition of $X^{p-1} - u$ into irreducible factors over $\mathbf{F}_p$.

□

Solution to Exercise 100**.**
For $p = 2$, we have $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

Assume p odd. Then $X^{p+1} - 1$ is the product of $(X-1)(X+1)$ by $(p-1)/2$ quadratic polynomials $X^2 + aX + 1$ where a ranges over the set of elements in $\mathbf{F}_p$ such that $a^2 - 1$ is not a square modulo p.

Notice that for any root we have $x^{p^2} = x$, with $x \in \mathbf{F}_p$ if and only if $x = \pm 1$, while and if $x \notin \mathbf{F}_p$ then its irreducible polynomial over $\mathbf{F}_p$ is

$$(X - x)(X - x^p) = X^2 + aX + 1$$

with $a = x + x^p$ and the discriminant $a^2 - 4$ is not a square. Conversely, if x is a root of such a polynomial, then its norm is $x^{p+1} = 1$. □

Solution to Exercise 101**.**
Let $(x, y) \in \mathbf{F}_8^2$ satisfy $x^3y + y^3 + x = 0$. If $x = 0$ the $y = 0$. If $y = 0$ then $x = 0$. Assume $(x, y) \neq (0, 0)$. Then $x \neq 0$ and $y \neq 0$. Write $\mathbf{F}_8 = \mathbf{F}_2(\alpha)$ with $\alpha^3 = \alpha + 1$ (see example 51). We can write

$$y = \alpha^j, \qquad x = \alpha^{3j}\beta$$

with $0 \leq j \leq 6$ and $\beta \in \mathbf{F}_8^\times$. We deduce

$$\alpha^{10j}\beta^3 + \alpha^{3j} + \alpha^{3j}\beta = 0.$$

Since $\alpha^7 = 1$, dividing by α^{3j}, we get

$$\beta^3 + \beta + 1 = 0,$$

hence β is a Galois conjugale to α. Since α has three conjugate, we obtain 21 points in $(F_8^\times)^2$. Counting the point $(0, 0)$, we conclude that there are 22 solutions in $\mathbf{F}_8^2$.

`Remark.` *The curve $X^3Y + Y^3 + X = 0$ is an affine version of Klein quartic*

$$X^3Y + Y^3Z + XZ^3 = 0.$$

□

Solution to Exercise 102**.**
`Hint:` use a software like Sage. See also the examples and exercise:

p	r	n	Reference
2	1	2	22, 50
3	1	2	52
5	1	2	
7	1	2	
2	1	3	51
3	1	3	64
2	2	2	67
3	2	2	
2	3	2	

□

Solution to Exercise 103**.** (see Example 58).
If $q \equiv 1 \bmod 5$, the polynomial $\Phi_5(X) = X^4+X^3+X^2+X+1$ splits completely in $\mathbf{F}_q$ into a product of 4 degree 1 polynomials, the polynomial X^5-1 is a product of 5 irreducible polynomials, therefore, it has $2^5 = 32$ divisors, 1 of degree 0 and 1 of degree 5, 5 of degree 1 and also 5 of degree 4, 10 of degree 2 and 10 of degree 3.
If $q \equiv -1 \bmod 5$, the polynomial Φ_5 is a product of two irreducible degree 2 polynomials in $\mathbf{F}_q[X]$, X^5-1 is a product of 3 polynomials, hence, it has $2^3 = 8$ monic divisors, 1 of degree 0 and 1 of degree 5, 1 of degree 1 and also 1 of degree 4, 2 of degree 2 and 2 of degree 3.
If $q \equiv 2$ or $3 \bmod 5$, the polynomial Φ_5 is irreducible in $\mathbf{F}_q[X]$, X^5-1 is a product of 2 polynomials, hence, it has $2^2 = 4$ monic divisors, they have degree 0, 1, 4 and 5.

Number of cyclic codes of length 5 *and of a given dimension over* $\mathbf{F}_q$

dimension	0	1	2	3	4	5
$q \equiv 1 \bmod 5$	1	5	10	10	5	1
$q \equiv -1 \bmod 5$	1	1	2	2	1	1
$q \equiv 2$ or $3 \bmod 5$	1	1	0	0	1	1

□

Solution to Exercise 104**.**
From Theorem 79 with $r = 2$ and $t = 1$, one deduces that if there is a 1–error correcting code on $\mathbf{F}_{q^n}$ of dimension r, then $1+n(q-1) \leq q^{n-r}$. For $q = 2$ this is $n \geq n_r$.

For $r = 1$ we have $n_1 = 3$ and the corresponding code on $\mathbf{F}_{2^3}$ of dimension 1 is the repetition code of example 71.

For $r = 2$ we have $n_2 = 5$ and a binary 1–error correcting code of length 5 and dimension 2 is the code of example 73.

For $r = 3$ we have $n_2 = 6$ and a binary 1–error correcting code of length 6 and dimension 3 is the code of example 74.

For $r = 4$ we have $n_2 = 7$ and a binary 1–error correcting code of length 7 and dimension 4 is Hamming's code of example 75.

□

Solution to Exercise 105**.**
From Theorem 79 with $q = 3$, $r = 2$ and $t = 1$, one deduces that if there is a 1–error correcting code on $\mathbf{F}_{3^n}$ of dimension 2, then $1 + 2n \leq 3^{n-2}$, hence, $n \geq 4$.

An example of a ternary 1–error correcting code of length $n = 4$ and dimension 2 is given in Exercise 106. □

Solution to Exercise 106**.**
(a) This ternary code has length 4, dimension 2, the number of elements is $3^2 = 9$, the elements are

$$\begin{array}{lll} (0,0,0,0) & (0,1,1,-1) & (0,-1,-1,1) \\ (1,0,1,1) & (1,1,-1,0) & (1,-1,0,-1) \\ (-1,0,-1,-1) & (-1,1,0,1) & (-1,-1,1,0) \end{array}$$

(b) Any non–zero element in $\mathcal{C}$ has three non–zero coordinates, which means that the minimum weight of a non–zero element in $\mathcal{C}$ is 3. Since the code is linear, its minimum distance is 3. Hence, it can detect two errors and correct one error. The Hamming balls of radius 1 centered at the elements in $\mathcal{C}$ are pairwise disjoint.

Recall that a MDS code is a linear code $\mathcal{C}$ of length n and dimension d for which $d(\mathcal{C}) = n + 1 - d$. Here $n = 4$, $d = 2$ and $d(\mathcal{C}) = 3$, hence, this code $\mathcal{C}$ is MDS.
(c) The elements at Hamming distance ≤ 1 from $(0,0,0,0)$ are the elements of weight ≤ 1. There are 9 such elements, namely the center $(0,0,0,0)$ plus $2 \times 4 = 8$ elements having three coordinates 0 and the other one 1 or -1:

$$\begin{array}{llll} (1,0,0,0), & (-1,0,0,0), & (0,1,0,0), & (0,-1,0,0), \\ (0,0,1,0), & (0,0,-1,0), & (0,0,0,1), & (0,0,0,-1). \end{array}$$

A Hamming ball $B(\underline{x}, 1)$ of center $\underline{x} \in \mathbf{F}_3^4$ and radius 1 is nothing but the translate $\underline{x} + B(0,1)$ of the Hamming ball $B(0,1)$ by $\underline{x}$, hence, the number of elements in $B(\underline{x}, 1)$ is also 9.
(d) The 9 Hamming balls of radius 1 centered at the elements of $\mathcal{C}$ are pairwise disjoint, each of them has 9 elements, and the total number of elements in the space $\mathbf{F}_3^4$ is 81. Hence, these balls give a perfect packing: each element in $\mathbf{F}_3^4$ belongs to one and only one Hamming ball centered at $\mathcal{C}$ and radius 1.
For instance, the unique element in the code at distance ≤ 1 from $\underline{x} = (1,0,-1,1)$ is $(1,0,1,1)$. □

Solution to Exercise 107**.**
The class of 3 in $(\mathbf{Z}/7\mathbf{Z})^\times$ is a generator of this cyclic group of order $6 = \phi(7)$:

$$(\mathbf{Z}/7\mathbf{Z})^\times = \{3^0 = 1,\ 3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5\}.$$

The condition $q \equiv 3 \bmod 7$ implies that q has order 6 in $(\mathbf{Z}/7\mathbf{Z})^\times$, hence, Φ_7 is irreducible in $\mathbf{F}_q[X]$. The polynomial $X^7 - 1 = (X-1)\Phi_7$ has exactly 4 monic divisors in $\mathbf{F}_3[X]$, namely

$$Q_0(X) = 1, \quad Q_1(X) = X - 1,$$
$$Q_2(X) = \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \quad Q_3(X) = X^7 - 1.$$

Hence, there are exactly 4 cyclic codes of length 7 over $\mathbf{F}_q$.

The code $\mathcal{C}_0$ associated to the factor $Q_0 = 1$ has dimension 7, it is the full code $\mathbf{F}_q^7$ with q^7 elements. A basis of $\mathcal{C}_0$ is any basis of $\mathbf{F}_q^7$, for instance, the canonical basis. The space of linear forms vanishing on $\mathcal{C}$ has dimension 0 (a basis is the empty set). The minimum distance is 1. It cannot detect any error. Since $d(\mathcal{C}) = 1 = n + 1 - d$, the code $\mathcal{C}_0$ is MDS.

The code $\mathcal{C}_1$ associated to the factor $Q_1 = X - 1$ has dimension 6, it is the hyperplane of equation $x_0 + \cdots + x_6 = 0$ in $\mathbf{F}_q$, it has q^6 elements. Let $T : \mathbf{F}_q^7 \to \mathbf{F}_q^7$ denote the right shift

$$T(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (a_6, a_0, a_1, a_2, a_3, a_4, a_5).$$

A basis (with 6 elements, as it should) of $\mathcal{C}_1$ is

$$\begin{array}{lllllllll}
e_0 = & & (1, & -1, & 0, & 0, & 0, & 0, & 0), \\
e_1 = & Te_0 = & (0, & 1, & -1, & 0, & 0, & 0, & 0), \\
e_2 = & T^2e_0 = & (0, & 0, & 1, & -1, & 0, & 0, & 0), \\
e_3 = & T^3e_0 = & (0, & 0, & 0, & 1, & -1, & 0, & 0), \\
e_4 = & T^4e_0 = & (0, & 0, & 0, & 0, & 1, & -1, & 0), \\
e_5 = & T^5e_0 = & (0, & 0, & 0, & 0, & 0, & 1, & -1).
\end{array}$$

Notice that $T^6e_0 = (-1, 0, 0, 0, 0, 0, 1)$ and

$$e_0 + Te_0 + T^2e_0 + T^3e_0 + T^4e_0 + T^5e_0 + T^6e_0 = 0.$$

This is related to

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = \Phi_7(X) = \frac{X^7 - 1}{X - 1}.$$

The minimum distance of $\mathcal{C}_1$ is 2, it is a MDS code. It can detect one error (it is a parity bit check) but cannot correct any error.

The code $\mathcal{C}_2$ associated to the factor Q_2 has dimension 1 and q elements:

$$\mathcal{C}_2 = \{(a, a, a, a, a, a, a) \ ; \ a \in \mathbf{F}_q\} \subset \mathbf{F}_q^7.$$

It is the repetition code of length 7, which is the line given by the equations

$$X_1 = X_2 = X_3 = X_4 = X_5 = X_6 = X_7$$

spanned by $(1, 1, 1, 1, 1, 1, 1)$ in $\mathbf{F}_q^7$, there are q elements in the code. It has dimension 1, its minimum distance is 7, hence, is MDS. It can detect 6 errors and correct 3 errors.

The code $\mathcal{C}_3$ associated to the factor Q_3 is the trivial code of dimension 0, it contains only one element, a basis is the empty set, a basis of the space of linear forms vanishing on $\mathcal{C}_3$ is $x_0, x_1, x_2, x_3, x_4, x_5, x_6$. Its minimum distance is not defined, it is not considered as a MDS code. □

References

[1] W. Chen – *Discrete Mathematics*, 201 pp. (web edition, 2008).
http://rutherglen.science.mq.edu.au/wchen/lndmfolder/lndm.html/

[2] M. Demazure, *Cours d'algèbre*, Nouvelle Bibliothèque Mathématique [New Mathematics Library], 1, Cassini, Paris, 1997. Primalité. Divisibilité. Codes. [Primality. Divisibility. Codes].

[3] D. S. Dummit & R. M. Foote, *Abstract algebra*, John Wiley & Sons Inc., Hoboken, NJ, third ed., 2004.

[4] M. Hindry, *Arithmetics. Primality and codes, analytic number theory, Diophantine equations, elliptic curves. (Arithmétique. Primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques.)*, Paris: Calvage et Mounet. xvi, 328 p. EUR 40.00, 2008.

[5] S. Lang – *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002.
In French: *Algèbre*, troisième édition, Dunod, 2004.

[6] R. Lidl & H. Niederreiter – *Introduction to finite fields and their applications*, Cambridge Univ. Press, 1994.
http://www.amazon.com/gp/reader/0521460948/ref=sib_dp_ptu#reader-link

[7] G.L. Mullen, C. Mummert – *Finite Fields and Applications*, Student mathematical library, **41**, AMS 2007.

[8] V. Shoup – *A Computational Introduction to Number Theory and Algebra* (Version 2) second print editon, Fall 2008.
http://shoup.net/ntb/

Michel WALDSCHMIDT
Université P. et M. Curie (Paris VI)
Institut de Mathématiques CNRS UMR 7586
Théorie des Nombres Case 247
F–75005 PARIS
e-mail: mailto:miw@math.jussieu.fr
URL: http://www.math.jussieu.fr/~miw/